IEEE Information Theory Society Newsletter

Vol. 49, No.3, September 1999 Editor: Kimberly Wasserman ISSN 1059-2362

Robert G. Gallager Wins the 1999 Harvey Prize

The American Society for the Technion-Israel Institute of Technology has named Robert G. Gallager, Professor of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology, the recipient of the 1999 Harvey Prize in the field of Science and Technology "in recognition of his fundamental contributions to information theory, and for his contributions to the theory of communication networks." The prize is one of two given annually, and consists of a cash award of $35,000 and the opportunity to lecture at the Technion. The Harvey Prize, established in 1972 by the late Leo M. Harvey of Los Angeles, honors major contributions to progress in science, technology, and medicine, as well as to advancement of peace in the Middle East. The first winner of this prize was Claude Shannon in 1972. Since 1990, three winners have received the Nobel Prize: Claude Cohen-Tannoudjhi (physics-1997), Pierre Giles de Gennes (physics-1992), and Bert Sakmann (medicine-1992). The prize was presented in Israel on June 16, 1999.

Prof. Gallager receiving the Harvey Prize. Left to right: Prof. Adrian Segal, Prof. Israel Bar-David, Prof. Robert Gallager, Prof. Jacob Ziv, and Prof. Abraham Lempel.

At the request of the editor, Dave Forney held the following interview with Bob Gallager in honor of his receipt of the prize.

Forney: Bob, congratulations on winning the Harvey Prize! We were talking a while ago about your early life and education, and I wonder if there was anything that you feel was particularly important along the way?

Gallager: I don't know how important any of it is, but it might be helpful to new people in the field to understand what a random path I took. When I was young, I had very little intention of becoming a scientist or engineer. When I went to college at the University of Pennsylvania, I went into electrical engineering primarily because I lacked aptitude for languages. EE was the only course I could take that didn't require foreign languages. I enjoyed the mathematics much more than the engineering, but found that when I was in classes with math students, I tended to think a little more like an engineer than most of them. I kept trying to understand what was going on at an intuitive level. One of the things that I've noticed about myself is that I don't deal easily with the abstractions of pure mathematics, but also I dislike the plethora of detail in many engineering problems. Trying to thread the path between abstraction and messy detail has pretty much defined the path that I have followed.

I did well academically as an undergraduate, but didn't take my studies very seriously. After my Bachelor's degree, I went to Bell Labs, because that was where all the action in communication was at the time. I started at the princely salary of $350 a month (not bad at the time). Bell Labs had an internal school called Kelly College for new engineers, which was probably the best place in the world to study communication at the time. I remember being taught by Dave Slepian, John Tukey and Bill Bennett.

After a year and a half, I was drafted into the U.S. Army. My unit had people drafted out of the Atomic Energy Commission, Bell Labs, and graduate schools every-

Continued on page 26

From the Editor

Kimberly Wasserman

In this issue of the IEEE Information Theory Society Newsletter, I hope you'll enjoy the feature interviews with Robert Gallager, winner of the 1999 Harvey Prize, conducted by G. David Forney, and James Massey, winner of the 1999 Marconi Fellowship Award, conducted by Bixio Rimoldi. I also hope you'll enjoy the columns by IT Society President Ezio Biglieri and Historian Anthony Ephremides, as well as Sol Golomb's puzzle column. In addition, there are announcements of prestigious awards recently won by members of our Society.

Please help me to make the Newsletter as interesting and informative as possible by offering suggestions and contributing news. The deadlines for the next few issues are as follows:

Issue	Deadline
December 1999	October 15, 1999
March 2000	January 15, 2000
June 2000	April 15, 2000
September 2000	July 15, 2000

Electronic submission, especially in LaTeX format, is encouraged.

I may be reached at the following address:

Kimberly Wasserman
Electrical Engineering and
Computer Science Department
University of Michigan
Ann Arbor, MI 48109-2122, USA
Tel: +1 (734) 647-3524
Fax: +1 (734) 763-8041
e-mail: wass@eecs.umich.edu

Kimberly Wasserman

IEEE
Information Theory Society Newsletter

IEEE Information Theory Society Newsletter (USPS 360-350) is published quarterly by the Information Theory Society of the Institute of Electrical and Electronics Engineers, Inc.

Headquarters: 3 Park Avenue, 17th Floor, New York, NY 10016-5997.

Cost is $1.00 per member per year (included in Society fee) for each member of the Information Theory Society. Printed in the U.S.A. Periodicals postage paid at New York, NY and at additional mailing offices.

Postmaster: Send address changes to IEEE Information Theory Society Newsletter, IEEE, 445 Hoes Lane, Piscataway, NJ 08854.

Table of Contents

James L. Massey Wins 1999 Marconi International Fellowship Award

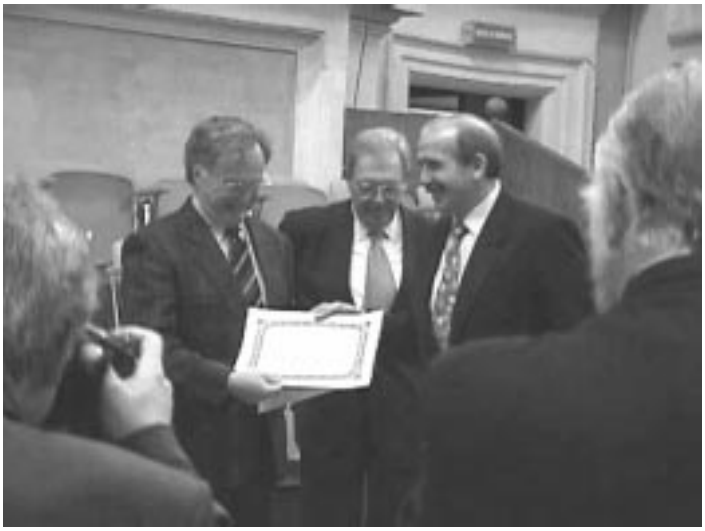
The Marconi International Foundation has named James L. Massey, Professor Emeritus of Digital Techniques at the Swiss Federal Institute of Technology (ETH) in Zurich, and Adjunct Professor at the University of Lund, Sweden, the recipient of the 1999 Marconi International Fellowship Award "for theoretical and practical contributions to cryptography and related coding problems; teacher and mentor to a generation of scientists and technologists." The award honors the name of Guglielmo Marconi, wireless inventor and entrepreneur, and recognizes creative work in communications science or technology and its benefits to humanity. The award consists of $100,000 and a work of sculpture. The award was presented in Marconi's birthplace of Bologna, Italy, on April 25th, 1999, the 125th anniversary of his birth.

At the request of the editor, Bixio Rimoldi held the following interview with Jim Massey in honor of his receipt of the award.

Bixio: When I think of Jim Massey I think of a person of unusual breadth and depth for all aspects of life. Your significant scientific contributions cover a wide spectrum. Some of your inventions have become industry standards. You have created two successful startup companies. You are often referred to as an exemplary advisor and teacher. In social events you appear as someone who really enjoys life. To excel in any of the above areas it would be quite normal to have to invest most of one's time and energy. To the contrary it seems that you always have time for people or to take up a new responsibility. What is your secret?

Jim: I think your statement here at the beginning is a gross exaggeration of my accomplishments. I had some small parts in many of these things, but I can say that it is generally true that I do enjoy life and in fact I have always made it a point to do what I thought was fun to do. Many times young researchers have asked me what problems they should be looking at and I have answered, "Well, what interests you? What is it that you would really like to work on?" I think that is more important than what *seems* to be important to work on. All of us have within us a voice that says this is interesting and we should look at it. If we follow that voice in the long run we will be happier and more successful than if we deliberately try to shape our work in a direction that seems to be important at the moment.

Jim Massey during acceptance speech.



Left to right: Jim Massey, Dr. Fabrizio Serena, Vice Chairman, Marconi International Fellowship Foundation, and the Hon. Jose Maria Jil-Robles, President, European Parliament, presenting the award.

Bixio: Is that attitude something natural to you or was it brought about by the environment in which you grew up?

Jim: Well, it is difficult to say where this attitude came from. Maybe I should discuss a little my education. I had the privilege of going to a Benedictine high school, i.e., a gymnasium in the European sense, that was very good. So I had a head start at the university. I have a twin brother, Jerry, and we both went to the University of Notre Dame. We both began in engineering but after one year Jerry switched to mathematics and after another semster to philosophy, which is where he has stayed ever since. He is now a professor of philosophy at the University of Pittsburgh. I went to military service immediately after the university, but Jerry did some graduate studies first. I spent three years on active duty in the Marine Corps, which was necessary to support the cost of my education at Notre Dame. We both had taken naval ROTC [Reserve Officer Training Corps] scholarships because our family could never have afforded to pay the costs of Notre Dame, even if those were much less than now. But I don't regret the time spent in the Marine Corps because I learned a lot of things there. Nothing technical, but a lot about dealing with people and what the rest of the world is like, things you don't see if you always remain in the same social stratus as you grew up in. I should mention that the electrical engineering education at Notre Dame was, in my opinion, very poor during the years I was there, 1952 to 1956. This contrasts, for example, with the education in mathematics which was very good. The best mathematics teacher I

Friends of information theory celebrating the 1999 Awardee at a restaurant near the Piazza Maggiore in Bologna. From left to right: Jim Omura, Susan Muroshige, Dick Blahut, Dave Forney, Lucretia Costello, Dan Costello, Israel Bar-David, Dahlia Bar-David, Barbara Blahut, Sohni Ungerboeck, and Gottfried Ungerboeck.

ever had was Vladimir Seidel at Notre Dame, from whom I really learned the notion of proof and the beauty of analysis. But the electrical engineering curriculum was definitely weak in general. It was always my feeling that even I could help out at Notre Dame. So I had decided if I could finish a Ph.D. program I would return to Notre Dame as a faculty member and see if I could help out the department there. I must say, not because of that, that today Notre Dame enjoys a very good Electrical Engineering department with people like Dan Costello and Tom Fuja, who are here at this meeting, [ITW, Kruger National Park} and Oliver Collins, people who are very well known in the Information Theory community.

Bixio: I have heard a funny story about you and Jerry being number one and number two at Notre Dame.

Jim: At Notre Dame at that time the grading system was a 0 to 100 points one so that a student's average was very finely quantized. It was possible to say exactly where you were in your class when you finished. When we finished in 1956 I was number one and Jerry was number two. I remember my average was 96.5 and his was 96.0 and that had the unfortunate feature for Jerry that he was labeled the "dumb Massey" and I was labeled the "smart Massey" from that point on.

Bixio: You and your twin brother Jerry must have been in constant competition. How did this impact your desire and ability to excel?

Jim: I don't think we were, Bixio. We never really competed with one another. I never had a sense that I was competing with him. In most of our schooling we were academically so far ahead of the others that it wasn't as if we were running a race with a lot of people in it.

Bixio: Do you have other brothers or sisters?

Jim: My sister always says that we never let anybody know that she exists. We have a sister who is three years older and now lives in Toledo, Ohio. A wonderful person, very bright, but she has never had any interest in an academic career.

Bixio: Do you see your desire and ability to excel as genetically determined or as a consequence of the upbringing?

Jim: I think that there certainly has to be an element of genetics in it. Children need a certain native intelligence in order to excel. If you are dealt a short deck, you are in trouble from the beginning. So I think we certainly profited genetically. I can also say we did not come from a family where scholarship was a tradition. We were the first in our family to go to the university. My mother supported us very much, but she had a hard life to raise the family because my father was killed at the end of the Great Depression when I was about seven years old. We were always poor if you measure things just in an economic sense. But we never felt poor. Maybe I didn't have a bicycle like other kids did but I never felt that it was such a bad thing. Probably it also helped that all three of us kids were very smart because the other kids, I am sure, envied that to some degree. But we were not bookworms. I never once took a book home when I was in primary school. Jerry never did either. It was too easy. In fact we went to a small Catholic school where there always were two grades in the room. We heard a year ahead of time what we were going to learn the next year.

Bixio: How did you decide to go into electrical engineering and communications in particular, and to go to MIT to do a Ph.D.?

Jim: I never knew what I wanted to do. The priests in my high school said: "Well, you are good in mathematics, you should go into electrical engineering." But I had no idea what an electrical engineer did. In my senior year at Notre Dame I had won a National Science Foundation fellowship for graduate studies and had decided then to go to the University of Illinois. It was the rule then that if you went into military service your NSF [National Science Foundation] fellowship was deferred until you returned from military service. Somehow, and I don't even really remember exactly the reasons why, when I was in the military service I decided I'd rather go to MIT. It was one of the best decisions in my life because, as you know, MIT at that time was the place to go for information theory. I almost aborted that chance because after my first year at MIT I was very disappointed with the place. It seemed like a big factory with so many graduate students. I actually applied to transfer to CalTech on a Hughes fellowship. Thanks to some lucky star I didn't get accepted into that program because if I did maybe I would be a solid state physicist today. It wasn't until my second year of doctoral study that I encountered information theory and fell in love with it. That love affair continues even today.

Bixio: Tell us about your encounter with information theory.

Jim: The first encounter was through Bob Fano's course "Transmission of Information" and then, of course, I later

got to know all the other people in the information theory group at that time. Jack Wozencraft was my thesis adviser and Jack had convinced me, not by advice but by example, that I should look into the communications area. I had an interesting course the first year from Irwin Jacobs who was teaching what we called the Davenport and Root course on stochastic processes. It was the first semester of my second year when I took Bob Fano's course and really got turned on by information theory. In the following semester I took Claude Shannon's course on advanced topics on information theory, which was fantastic. Besides those people, there were Bob Gallager and lots of other great information theorists, like Peter Elias, to have contact with. Aside from the faculty, there were many graduate students who are now well-known information theorists and we interacted a lot with one another.

Bixio: How was it to be a graduate student at MIT in those days?

Jim: There was a lot of mutual education among graduate students. We did not have private or semi-private offices. We were crowded into big rooms, we talked to one another, we knew what each other was doing, we helped each other out when we could. It was a very stimulating and interesting time. One thing I always regretted is that I didn't stay at MIT long enough. I was there only three years. I got my Masters degree after the first year and the doctoral degree after another two years. The reason was the wolf at the door. I was married and by the time I was finished I had two children and could not survive on the 250 $ / month that I was getting from the NSF. So I really made an effort to finish quickly. I have often felt it would have done me good to stay one or two more years in that environment, but I didn't have that opportunity.

Bixio: What difference did it make to have Shannon around?

Jim: Well, I profited directly from having Shannon there. He was a reader of my dissertation and he gave me some good advice on it. But I profited mostly by his example, from the way he looked at problems, which came across very clearly in his lectures: always simplifying, simplifying until you get it down to something that a human being can actually understand. Seeing the solution at that point became obvious and then you reintroduce complexity until you finally get the solution to the initial problem. That was very, very good. But I think one shouldn't misunderstand the environment at MIT. MIT is a very special place and it was very much the attitude at that time that all the interesting problems in information theory had been solved. Certainly there were no more problems left in coding because sequential decoding had been developed and analyzed to some degree and the BCH codes were then available. This was in 1961-1962. People thought, "Oh, there is nothing interesting left to do, particularly in coding" and I was advised not to attempt to do my thesis in the area of coding. But I liked coding too much. It was too much fun so I decided I was going to work on coding and it turned out to be a good decision.

Bixio: Your thesis on threshold decoding was an excellent career start. It received the IEEE Information Theory Society Paper Award and it also motivated the start of a company. Tell us about your thesis.

Jim: Basically my thesis came about from realizing that the "right" way to look at a convolutional code was simply as a discrete-time linear system. Once I started taking that viewpoint, making some system diagrams to compute syndromes, and looking at the equations that the syndromes were giving, I saw that many of these syndromes gave independent estimates of error bits. Then it was an easy step from there to threshold decoding in a more general sense. Also when you took that same viewpoint and went back to look at block coding, you saw more and more places where you could use the same idea. The idea is simple, one might say trivial, and I got a lot of mileage out of it. But I never worked on it again after that time.

The reason why Codex Corporation got started was actually a fluke, like many things in my life. One of the big defense companies in the US, Melpar, had located its research group in Watertown, Massachusetts. Melpar, for various reasons, maybe cost, decided at that point that they would close the facility in Watertown and move everybody down to the main headquarters of the company in Falls Church, Virginia. Most of these researchers were New Englanders and Bostonians and no way were they going to move. This was particular true of the best of them. So here suddenly you had a lot of very talented people who were unemployed and looking for something to do. They decided that they would form a new company to do something. Bob Gallager at that time was a consultant to Melpar so they knew about Bob's low-density parity check coding scheme. Bob had introduced me to Arthur Kohlenberg who was Chief Scientist at Melpar (and Editor of the IT Transactions). Kohlenberg had me come out to give a talk about threshold decoding. The Melpar people were interested in that because it seemed very practical. You could really build these systems with the hardware of the day. They decided that they would form a company with two objectives. The nearer range objective was to make threshold decoders because they knew they could make these quickly, and the longer range objective was to make low-density parity check coders and decoders. So the company was started in 1962 and I was given some stock in the company in exchange for patent rights. It worked out very nicely and as you know the company later became a division of Motorola—I think that was in 1977. Of course there were a lot of other people involved, preeminently Dave Forney, who came in later. Dave is junior to me by about 3 or 4 years. He decided rather than going to Bell Labs or other big research companies to come to Codex. He was extremely crucial to the success of the company. So Codex had all the time Bob Gallager and Dave. I occasionally went there but my contributions were much smaller than those of either of them. Still threshold decoders played an

Continued on page 22

President's Column

Ezio Biglieri

Ezio Biglieri

The objective of the IEEE Information Theory Society, says Article I of its Constitution, "shall be scientific, *literary*, and educational in character"(emphasis supplied). While this statement of our founding fathers obviously refers to our activities in publishing technical literature (more about this soon), I shall stretch its sense here to make the main point of this column, one that concerns the literary aspects of our technical writing.

One of the recent decisions made by the Board of Governors of our Society is to consider the possibility of sponsoring a series of translations into English of a number of information-theory books published in other languages. Contacts to this purpose were initiated with a handful of publishers, and we are now trying to identify a number of books whose translation may render a service to the information-theory community. If you have suggestions about any such book, please inform Han Vinck at vinck@exp-math.uni-essen.de

Now, let me introduce my point about technical writing. Not many years ago I had the occasion of meeting a famous historian who was just hired by my University. When I told him that I had had the occasion of reading a couple of his books, he commented that he felt guilty for not being able to reciprocate: he had tried several times to approach a technical book, but could never get much out of it. We both agreed that the blame about this deplorable asymmetry should be put on the "two cultures" paradigm in academics and thought, one that posits the humanities against the sciences, the "fuzzies" against the "techies." But at that time I also felt that we scientists write in a prose that is too dry, formal, and esoteric to be appealing to non-technical readers, and hence we should accept our fair share of responsibility for this situation.

Only later did I start changing my mind about technical writing, and shedding my inferiority complex with respect to the literary style of the humanities: I realized that difficult writing is sometimes necessary in scholarly work (even Socrates was mocked by Aristophanes, in "The clouds," for his technical language), that a scientific approach implies the existence and the use of a scientific vocabulary, and that if we define good writing as clarity and limpidity, then many of our writings should be classified as good. Yes, they are often tough on the reader, and require hard work and discipline to be penetrated. Yet, our "scientific jargon" is a powerful instrument, one which allows deep concepts to be expressed with a considerable economy of means and is not conducive to babble. Moreover, it does not perform well in writing only. On the contrary, as we experience in our everyday activities, it displays its considerable power even when we convey our ideas in informal talks and in conferences (at this point I cannot resist quoting a recent, Veblenian definition of a technical conference: it's "the leisure of the theory class"). Listen at Lee Smolin, a theoretical physicist at Pennsylvania State University: "One of the differences between the traditions of science and the humanities is that the humanities have become traditions of reading and writing. People in these fields don't talk to each other. They sit at home and they sit in their offices and they construct sentences and paragraphs, and they don't speak to each other. Scientists speak to each other, first and foremost. Our culture is verbal, and we know how to talk to people. Go to a talk given by somebody in philosophy or literary theory. Notice that they invariably will read something that they've written, word for word. Very few scientists will ever do that." (in John Brockman, "The Third Culture," 1996).

We may even claim that in many ways the technical language is superior to the language of the humanities. My bit of argument in support to this assertion comes from the observation of a recent trend in the humanities: as many of you might have experienced, their written work has a tendency to mimic technical writing in two ways: either (i) by using a literary structure borrowed from the scientific language (the need for a clear stipulation of the meaning of every single word used: recall Humpty Dumpty's statement that "when I use a word it means just what I choose it to mean —- neither more nor less") , or (ii) by using the rhetorical device of supporting a thesis by showing its analogy with a proven scientific fact (mostly taken from physics and mathematics, but specially chaos theory, quantum physics, complexity theory, and fractals). Now, the flip side of these procedures is that often (i) only the negative aspects of technical writings are reproduced, and (ii) the scientific facts are not well understood.

Concerning point (i), sometimes writing is just made more obscure: as the British Nobelist Peter Medawar puts it, "There are some fields that are genuinely difficult, where if you want to communicate you have to work really hard to make the language simple, and there are other fields that are fundamentally very easy, where if you want to impress people you have to make the language more difficult than it needs to be." (*op. cit.*). No doubt there exist thoughts so profound that most of us will not understand the language in which they are expressed (try to read Martin Heidegger without a training in philosophy). However, there is also language made unintelligible on purpose, so as to conceal an absence of clear thought. Which does not go totally unnoticed among scholars in the humanities, though: the journal *Philosophy and Literature* holds an annual Bad Writing Contest, with prizes going to top scholars. Excerpt from a recent

winner: "If such a sublime cyborg would insinuate the future as post-Fordist subject, his palpably masochist locations as ecstatic agent of the sublime superstate need to be decoded as the 'now-all-but-unreadable DNA' of a fast deindustrializing Detroit, just as his Robocop-like strategy of carceral negotiations and street control remains the tirelessly American one of inflicting regeneration through violence upon the racial heteroglossic wilds and others of the inner city." There is even an Internet site that automatically creates a jargon-filled, incomprehensible "post-modern'' essay every time someone logs onto it (www.cs.monash.edu.au/cgi-bin/postmodern). I tried it, and obtained a long essay that includes the statement "In the works of Gibson, a predominant concept is the distinction between without and within. Any number of constructions concerning a self-falsifying whole exist. The subject is contextualised into a rationalism that includes art as a totality."

As for the use of scientific facts to support philosophical or sociological statements, a recent story tells about its risks. In 1996, Alan Sokal, a New York University physicist, tricked the journal *Social Text* into publishing a parody of a philosophical essay as a serious article. Its title was "Transgressing the boundaries: Towards a transformative hermeneutics of quantum gravity." This article used (imaginary) recent findings about a quantum theory of gravity to support some tenets of postmodern ideology. From start to finish the paper was pure gibberish: besides numerous half-truths, falsehoods and non sequiturs, this article contained even, in its author's words, some "syntactically correct sentences that have no meaning whatsoever". This work deservedly earned the 1996 IgNobel prize for literature. Later Alain Sokal and Jean Bricmont (the latter a professor of physics at the University of Louvain in Belgium) published a full book, entitled "Impostures Intellectuelles" in its original French edition, and "Fashionable Nonsense" in its American translation. In it, they condemned a number of well-known, well-respected authors who have invoked concepts from physics and mathematics to support their theses by "mixing them up arbitrarily and without the slightest regard for their meaning." The book is often hilarious. Read it, and you will learn, among other things, what the human erectile organ has to do with the square root of minus 1 (Lacan), that the poetic language is a non-denumerable set (Kristeva), or that the modern wars take place in a non-Euclidean space (Baudrillard).

Awards

Norman C. Beaulieu Wins E. W. R. Steacie Memorial Fellowship

The Natural Sciences and Engineering Research Council (NSERC) of Canada has announced that Norman C. Beaulieu is one of the recipients of the 1999 E. W. R. Steacie Memorial Fellowship awards. The award recognizes university researchers who have captured international attention for outstanding scientific or engineering achievement. Dr. Beaulieu is the first electrical engineer in 15 years, and only the fifth electrical engineer in 35 years, to receive the award. Dr. Beaulieu is a Professor of Electrical and Computer Engineering at Queen's University, Kingston, Canada.

From left: The Honourable Ronald J. Duhamel, Secretary of State of Canada, Norman C. Beaulieu, and Dr. Tom Brzutowsi, President of NSERC.

Shlomo Shamai Wins the 1999 van der Pol Gold Medal

The 1999 van der Pol Gold Medal has been awarded to Shlomo Shamai with the citation: "For contributions to the basic understanding of the potentials for and the limitations to information transfer through various communication channel models." The Medal and certificate will be handed over to Shlomo by a grandson and namesake of Balthasar van der Pol during the Opening Session of the URSI General Assembly in the Convocation Hall of the University of Toronto, on Sunday, 15 August 1999.

The Balthasar van der Pol Gold Medal is awarded by URSI(International Union of Radio Science) to an outstanding scientist whose achievements in any of the branches of science covered by the Commissions of URSI have been particularly valuable, and with evidence of significant contributions within the most recent six-year period. The award is presented at intervals of three years on the occasion of the General Assembly of URSI.

The Historian's Column

A. Ephremides

A. Ephremides

Today I am about to engage in a risky, but truly historical discussion. I am not going to confine my comments to the history of our Society; rather, I will talk about real History! Yet, the topic will be Communications, the main field on which Information Theory has had an impact.

At a recent workshop in Metsovo, Greece, I found the opportunity (tongue-in-cheek) to claim that the Ancient Greeks, in addition to discovering everything else under the sun, were the first real inventors of cryptography and compression. After all, didn't the original Trojan Horse mark the first time that stealth was used? And isn't the very name used today to describe unauthorized intruders who enter an information system? And, similarly, weren't the ancient Greeks the first to eliminate the "space" symbol from written text? And isn't this an elementary, yet genuine, form of compression?

I can sense your bemusement, if not irritation, already. Yet, there is more! I am about to raise the fundamental question of who invented the first form of telecommunication. And, I am about to argue that (guess what) it was the Ancient Greeks!

Of course, sight and sound are the natural means with which primitive man was endowed in order to communicate. And it is these means that are used even today. Except that we have developed sophisticated media that carry our signals to remote locations and we have improved tremendously the rate at which we can transmit them.

The first documented form of telecommunication can be found in Homer. To mark the fall of Troy and to inform Klytemnestra about it, there was a sequence of fire signals that were relayed from mountain-top to mountain-top from Troy to Mycenae. And it took twenty-four hours. To transmit one bit over twenty-four hours may not seem very impressive by today's standards, but it certainly beat transport via a messenger.

In fact this process of relaying a message via fire signals became very widespread in Ancient Times. The medium of relay via consecutive fire signals was termed "fryktoria", which literally means "sequence of burning sites." Think of it as a primitive optical wireless system; the first of its kind! Ample documentation of the use of these "fryktorias" (especially in military situations) can be found in Aeschylus's tragedies, notably "Agamemnon".

A significant improvement occured in the Hellenistic Period (~ 3rd century B.C.) when two engineers from Alexandria conceived the first coded communication system. They organized the twenty-four letters of the Greek Alphabet into a 5x5 table of rows and columns (with the 25th entry blank). Then, the transmitter used two white background stone-panels against which a fire signal could be lit. So, to transmit a letter, say "K", which is located at the second-row and fifth-column position in the table, a fire signal was flashed two times against the left wall and five time against the right wall, thus enabling the receiver to understand which letter was sent. Certainly, not exactly a portable system nor a very efficient one; yet it permitted remote communication of text; and that was more than two millenia ago!

A parallel invention that utilized sound media was developed at about the same time. It utilized a horn that was suspended from a scaffold of poles at about a height of four meters, in such a way, that it permitted a full 360-degree rotation. Thus, the signal could be sent in any direction, thereby marking the birth of the first omni-directional antenna.

A more elaborate system is reported a century, or two, later, that utilized the earth as the medium of transmission. Sound signals were imbued on rocky ground and they could be heard at reasonable distances that exceeded the range of sound traveling in the air.

Of course, these techniques were adopted widely by others and their use spread into the Roman era. The Romans added significaant enhancements but the basic idea remained the same. In fact, it remained the same for centuries until electricity was discovered and the first genuine telegraph was developed. The breakthrough brought about by the telegraph was not so much the increase in range which was modest, but, rather, the dramatic increase in rate. It can be argued that the transition from the line-of-sight optical transmission to the telegraph marked the beginnings of the information technology era. Then came Bell and Marconi, and .... Shannon! And the rest is ..., well, history.

It is interesting to note that the "mover-and-shaker" in promoting the development of telecommunication systems had been the military. It is remarkable that this has been true since ancient times. Perhaps the ... Internet is the first system that broke this tradition.

I hope you will agree that the Ancient Greek "fryktoria" qualifies as the first documented telecommunication system. But, the Ancient Greeks deserve even more credit. The very word "communication" ("epikoinonia", in Greek) carries with it the deeper meaning that permeated all of Ancient Greece's contributions to civilization. It describes the process by which people are organized into a "commune" or "koinonia" (i.e., Society). That is, it assigns to the "engineer-

ing" process, by means of the brilliantly chosen term "communication", the meaning and the purpose of this process. Thus, even though military needs pushed the state-of-the-art, the "art" itself had a loftier objective.

Well, I told you that this would be a risky undertaking. I hope that you see, however, that the description of the claims to greatness of the Ancient Greeks was done with objective detachment and in a highly professional, unbiased manner! And I am the first to tell you so!

In closing this escapade, I wish to give credit to the various exhibits in the Telecommunications Museum of the Hellenic Telecommunications Organization (OTE) in Athens, that provided the data and the motivation for this column.

IEEE Information Theory Society Board of Governors Meeting

Saturday, February 27, 1999,
Santa Fe, NM

Attendees: Andrew Barron, Vijay Bhargava, Ezio Biglieri, Michelle Effros, Anthony Ephremides, Thomas Ericson, Marc Fossorier, Alfred Hero III, Ralf Koetter, James Mazo, Steven McLauhglin, Greg Pottie, Ramesh Rao, Joseph O'Sullivan, Alexander Vardy, Sergio Verdu, Steve Wicker, Bin Yu, Ken Zeger

1. Welcome. The meeting was called to order by Ezio Biglieri at 8:45 AM. Introductions were made, and the new members were welcomed.

2. The agenda was approved.

3. The minutes of the meeting of August 1998 in Cambridge, MA, were approved.

4. New Appointments and Miscellaneous Announcements.

a) Jody O'Sullivan reported on the results of the Santa Fe workshop. Technical contributions were of high quality and sessions were well-attended with more than 80 registrants. The social events went well, and a small surplus of $2000 was generated. An NSF travel grant was secured, and support provided to 13 attendees. Sergio Verdu suggested that the BoG thank the organizers, which was met with a round of applause.

b) Ezio Biglieri proposed that the annual meeting be designated as South Africa. The BoG meeting will be the Sunday before the conference (June 20). Vijay Bhargava indicated that there will be BoG members who cannot stay for the whole conference, so this needs to be worked into the conference package. The third meeting of the year will be held in conjunction with the Allerton conference. Four options were suggested by Bruce Hajek. The meeting will start at 8:30 AM in Chicago on Saturday Sept. 25 for travel convenience.

c) ISIT is approaching 1000 member attendance, and organization is becoming increasingly difficult. Consequently, a briefing by Ms. Michael Ellis was invited on IEEE conferences. The briefing was held after lunch (see Addendum).

d) Information Theory Society members continue to be honored for their contributions. Wesley Peterson has won the prestigious Japan Prize. Kees Imminck won the IEEE Edison Medal. Vijay Bhargava won the IEEE Haraden Pratt Award. 13 IT members were elevated to Fellow status. The deadline for nominations for Fellow status for next year is March 15.

e) Marc Fossorier was appointed the new Treasurer with BoG consent, replacing Benhaam Aazhang, who is stepping down after three years of service. Kim Wasserman was appointed as the new editor of the newsletter.

5. The standing and ad-hoc committees were discussed. A list of the committees and their chairs is below.

Standing Subcommittees.

1. Nominations: Thomas Ericson
2. Constitution and bylaws: Sergio Verdu
3. Claude E. Shannon Award selection: Ezio Biglieri
4. Awards: Vijay Bhargava
5. Membership and Chapters: Joachim Hagenauer
6. Publications: Alexander Vardy
7. Fellows: Vincent Poor.

Ad Hoc Committees.

1. Workshops and Symposia: Tom Fuja
2. Distinguished Lecturer Program: Vijay Bhargava
3. Web Editor: Ramesh Rao
4. IEEE New Technology Directions: Stephen Wicker
5. PACE Liasion: David Brady
6. IEEE Press Liasion: Han Vinck
7. IEEE History Center Liasion: Anthony Ephremides
8. IT Books Translations: Han Vinck
9. Electronic submissions to IT conferences: Ramesh Rao

Sergio Verdu noted that there are some oddities in the bylaws and constitution (e.g. the President is an ex-officio member of the fellows committee, but is not necessarily a fellow). It was recommended that the awards committee be increased in size to 7-9. It was noted that a number of ad hoc committees might be converted into standing committees. (Ad Hoc committees must be approved each year). Discussion then turned to some newly proposed ad hoc committees.

a) Ad-hoc Committee on IT books translations. There are a number of good IT books in Japan, Russia, France, etc. which have not been translated into English. A barrier is that publishers need to buy translation rights, which means outlay of substantial funds up front. The idea is to have the Society

potentially provide some funds up front to see if IEEE Press or others can publish these. Han Vinck would head the committee. The committee will first look into costs, and suggest some candidate books for translation.

b) Ad-hoc Committee on electronic submissions to IT conferences. The idea is to construct standard forms to be used for future conferences. This way people do not need to reinvent the wheel each time, and will also accommodate new IEEE requirements on publications. This will be considered in the context of how the Society handles all of its electronic publications. Tony Ephremides mentioned that considerable work has been performed on this task by numerous conference organizers; we should draw on this experience.

6. IEEE Technical Activities Board.

Ezio Biglieri reported on the TAB Meeting of Feb. 1999 held in South Carolina. An e-mail report will be circulated among the BoG members. A "Best Practice" booklet is being produced by TAB based on their last Society review; this may have some good ideas for the IT Society. There will now be a late closing fee for conferences, in escalating amounts after 12 months. Thus conference organizers are urged to quickly close the books. There will be a panel of editors meeting in April. There is some pressure from IEEE in that the Society should provide more support to the Chapters. Societies should in particular support attendance of Chapter members at the Sections conference in October. Vijay Bhargava moved that a letter be sent to all Chapter chairs inviting them to go the conference, with an offer of partial support. The motion carried. It was also reported that TAB is considering new financial models for operation of Societies.

7. Treasurer's Report.

The net worth of the Society is $1.295 M. Some questions were raised as to how net worth related to long-term investments, which are now valued at $1.148 M. The BoG consensus was that in the future, reports should also show our current accounts, and that a more transparent and detailed format be used. Ramesh Rao raised the issue of mailing costs for the Transactions; this will have effect on electronic publishing decisions.

8. IEEE Information Theory Society Web Site and Digital Library.

Ramesh Rao reported the IT web site has been hacked and attacked several times, and so UCSD has been putting in new security measures that as a side effect make management more difficult. The digital library demands much more resources than the IT website, and thus it was proposed to consolidate the sites to make it more convenient to manage. Presently, the Society is not providing ongoing support for the costs of maintaining these sites. The digital library searching functions are up, and abstracts have been rendered in pdf. Marketing of this product to institutional customers and the members at large will need more than a volunteer structure. IEEE might need to be involved because of policy implications in publishing. Total cost would likely be $36K per year for professional management of the site, which is roughly $5 per member. This is a difficult issue in that much of the revenue from publications comes from institutional customers. Finding an appropriate funding mechanism needs to be made. IEEE is in general technically behind the IT and SP societies, and so we will be largely on our own in charting this course. One suggestion was to approach advertisers for the site. There was considerable disagreement on the merits of such a scheme. There was also discussion on whether we should use web-based services, or send out CDs as the preferred electronic format. Another option is to provide a means for members to be able to decide whether to go completely electronic, with a difference in price between receiving both electronic and paper copies. It was suggested that we send a letter to our members to educate them on the options and request feedback. Consensus is that we must in the short term continue having paper copies for everyone, and then consider various options (CDs, web sites) at a variety of prices. Further discussion on this very important issue will take place at successive BoG meetings.

9. IEEE Information Theory Society Newsletter.

Michelle Effros reported. The March issue has been prepared by the new editor, Kimberly Wasserman. The editor has an archive going back to the late 70s for newsletters. IEEE has no archive, and in fact destroys back issues within a year (they continue to be available on microfilm only). Questions were raised as to how the Society will archive its publications and other materials; a suggestion was made for a role for the IEEE History Center.

10. IEEE Transactions on Information Theory Report.

Alexander Vardy reported on a number of issues.

a) Electronic submission and tracking. This was approved by the BoG in June; already 28% of submissions are electronic, even though many authors are unaware of this option. Eventually we would like almost the entire editing and review process to be electronic. Tracking is now available to the Associate Editors.

b) Growth of the Transactions. There was large growth in '98 due mainly to the special issue.

c) Publication Schedule and Reference Index. The reference index uses up 150 pages, and produces a considerable publication delay. The author and subject index do not cause problems. Sergio Verdu moved that the reference index will not be published, but the Editor in Chief will ensure that it still be compiled electronically for use in the Society website. The motion carried. A note on how to access this information will appear in the November issue.

d) Paper loads. The top five loaded associate editor positions were in coding theory, and so it was recommended that one more associate editor position be created in this area. Patrick Sole will be the new editor. It was also recommended that Marcello Weinberger succeed Neri Merhav effective July 1, 1999. Both recommendations received Bog approval. There was some discussion about possibly formalizing a breakdown

of topic areas among the editors, but in the end it was decided that the Editor in Chief retain discretion in this area.

e) Archiving of supplementary material papers. An issue was raised by a contributor to the Transactions as to whether there should there be an electronic archival site for materials that cannot appear in papers, to be maintained by the Society. This might include for example simulation code, large tables, and the like. The consensus from the resulting discussion is that the Society should only archive material that has gone through peer review, and that in general papers must be self-contained, reaffirming present practice. Electronic materials can be referenced by the authors of a paper, where appropriate.

10.1 Publications Editor report and transition.

Steve McLaughlin reported that IEEE is doing a version of Inspec, which may have an impact on our digital library; moreover there will be restrictions on conferences so that their proceedings can be linked to the new structure. The IEEE Press reprint of the Oct. 98 issue will include a CD that has an index of the electronic library plus contents of the book. It is expected that the book will be published in June or July. A round of applause was given for the job Steve has done over the years.

10.2 Discussion of the proposed 2001 special issue (Proposed Editors: Forney, Frey, Koetter, McEliece, Spielman).

Ralf Koetter proposed a special issue on codes, graphs, and iterative algorithms. This would include belief propagation, turbo-decoding, gradient search, and variations, with a target date of April 2001, and a page count of around 400. There will be a workshop on this topic in the preceding summer. The special issue was approved. Vijay Bhargava brought up a policy question on how committees and editorship of special issues are determined, with the view to seeing more participation from the Asian-Pacific and European/Middle East regions. This should be considered at the beginning of all such processes, to try insofar as possible broaden points of view while maintaining high quality.

10.3 Proposed Special Issue for 2002. (Proposed Editors: Landau, Mazo, Shamai, Ziv).

Jim Mazo proposed that this issue be prepared for April 2002, as a tribute to Aaron Wyner, on the topic of Shannon Theory: Perspectives, Trends, and Applications. Both invited and submitted papers will be used. There will be a front page with a dedication. Vijay Bharagava moved that the publication be approved. The motion carried.

10.4 Proposal for another Publications Editor position.

The Transactions have increased considerably in page count since the position of Publications Editor was created 10 years ago, to the point where it is difficult for one volunteer. The division of duties would be determined by the two publications editors in consultation with the editor-in-chief. The cost is roughly 4-5K per year for staff support. A motion to accept the recommendation carried.

11. Electronic publication.

Thomas Ericson observed that much time has been devoted to policy issues surrounding electronic publications, and we can only expect this topic area to become increasingly important. We must both try to stay at the forefront, and be sure that any undertakings can be followed through. He suggested the creation of an ad hoc committee to discuss the policy issues for electronic publications for presentation at BoG meetings. A formal proposal will be made at the next meeting.

12. Ad-hoc Committee on IEEE New Technology Directions.

Steve Wicker reported that the TAB ad-hoc committee has been looking at new technologies that may have implications for the IEEE. Societies have been submitting one-liners on new or emerging technologies. Solicitation of this from BoG members will take place via email.

An earlier report prepared by TAB was used by granting agencies, and thus we need to provide timely input.

13. Distinguished Lecturer Program.

Vijay Bhargava reminded the BoG any past or present member of the board is defined as distinguished. Up to $500 in expenses can be defrayed from talks to Chapters. Not many people have taken advantage of this so far, but it could be an important element of increased activity in chapters.

14. Symposia and Workshops [Document 4]

a. 1998 Workshop on Information Theory, San Diego, CA.

Ken Zeger reported that the receipts were were $75K, outlays $72K, and a check will shortly be going to the Society. The books should be closed within the one year deadline.

b. ISIT 1998, Cambridge, MA.

Sergio Verdu reported on some results. Feedback to the organizers was that people generally liked having no long papers, and having things posted on website beforehand. The conference has a surplus of around $38K. The final financial report has been prepared.

c. 1999 Information Theory Workshop, Kruger National Park, SA.

There was no report beyond the matter of the BoG meeting mentioned above.

d. 1999 Workshop on Information Theory and Networking, Metsovo, Greece.

Tony Ephremides reported that everything is on track

e. ISIT 2000, Sorrento, Italy, June 25 - June 30, 2000

Ezio Biglieri reported that the budget has been approved by IEEE, and room bookings have been made. The costs will be roughly $100 per person on double occupancy for four star hotels, and $60 per person for 3 stars. They are looking into arranging bungalows at a campsite for students and budget travellers.

f. ISIT 2001, Washington DC, USA, Date TBD.

Tony Ephremides circulated a report on behalf of the organizers. Downtown hotels are being considered, and they are

working on getting a conference service organization. They are assembling the complete committees. A large program committee (70 people) is being assembled so that all reviews are done internally rather than finding others outside. There was considerable discussion on this point, which reached no definite conclusion. The organizers will be invited to discuss the matter at the next BoG meeting.

g. ISIT 2002.

Hideki Imai prepared a preliminary proposal for ISIT 2002 in Yokohama, Japan, which was presented by Michelle Effros. A September date was suggested to avoid conflict with the World Cup. Discussion on the proposal suggested that the organizers consider less grand venues (increasing the options during the World Cup run-up) and a time frame of late June, to bring the ISIT closer to the target dates approved in a prior BoG meeting.

15. Awards Committee.

The paper awards nomination deadline is April 15. The committee will work mainly by email to produce a recommendation three weeks in advance of June BoG meeting.

16. IT Society Logo.

The logo is being modified to be included in the Transactions.

17. New Business.

Sergio Verdu raised the issue of the causes of delays in publishing papers in the Transactions. It was requested that more statistics on delays between submission and response in reviews be collected, with a breakdown by associate editors. This is felt to be easier now that we have a tracking database. There was general agreement with the suggestion.

18. The meeting adjourned at 12:58 PM.

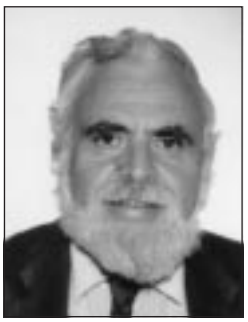
Addendum: IEEE Conference Services Presentation by Ms. Michael Ellis.

A viewgraph presentation was made, to outline the professional support services available to organizers of IEEE sponsored conferences. Customized meeting plans, on-line registration, on-line travel, tax liability, looking into grants, help with site selection and contract negotiations are among the items offered (with varying fees depending on the options selected). For no fee, they will review contracts within 24 hours to be sure organizers are getting what they expect. Also since they do many conferences they can get discounts from national chains, both for hotels and services such as A/V, transportation, and decorating. The on-line registration also allows people to register to IEEE and particular Societies. They can deal with credit card, local currency, and checks even in foreign currency. The on line reservation system can get daily registration totals to control hotel expenses, and deal with room blocks at multiple hotels to route enough people to not have to pay penalties through attrition clauses. Conference management services include A/V, meals, rooms, review of invoices before they go to conference organizers, room monitoring, budget prep, investment of excess cash, monthly reports, closing reports within 90 days, pre-audit checklist, and banking. Database administration includes merging of addresses, clean up of addresses, maintenance of mailing list for $5k basically in perpetuity for management of the same conference. Technical program management includes login of abstracts and papers, author kits, processing CD-ROM preparation, advance and final program layout. They can also provide some tips to speakers on public presentations. The Web reservation system includes access to a travel service that can provide discounts for particular airlines, a database for IEEE members, and (through the travel office) provision of services such as looking for lowest prices and giving alternatives for travel. Organizers can pick and choose which services they want from IEEE, as the services are priced individually. However, organizers are strongly urged not to split pre- and on-site registration, due to predictable interface problems.

GOLOMB'S PUZZLE COLUMN™ PUZZLE NO. 47:

Find the Simple Solution

Solomon W. Golomb



This is an assortment of problems that I have collected from a variety of sources over many years. You may have seen some of these before. What they have in common is that each has a simple solution if you find the right way to look at it.

1. Cities A and B are 100 miles apart. At 9:00 a.m., one train starts out from A heading toward B at a constant speed of 40 mph, and another train starts out from B heading toward A (along the same track) at a constant speed of 60 mph.

   a. Also at 9:00 a.m., a fly takes off from the front end of the train departing from A, heading along the track toward B, at a constant speed of 75 mph. When it reaches the front end of the train which departed from B, it makes an instantaneous 180° turn, and continues at its constant speed of 75 mph, until it gets back to the front end of the train from A, where it makes

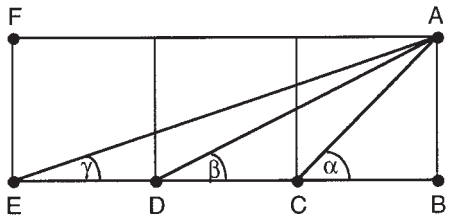
another instantaneous 180° turn. It continues in this fashion until the two trains meet. What is the total mileage logged by the fly on its back-and-forth voyage up to the time that the two trains meet?

b. A second fly starts out at the front end of the train departing from B at 9:00 a.m. in the direction of A, and flies at a constant speed of 50 mph, programmed with the same basic instructions as the first fly. What is the total mileage logged by this second fly up to the time that the two trains meet?

2. In one version of billiards, balls numbered from 1 to 15 are on the table top, and on the first player's turn, any one of the fifteen balls may be knocked off the table. Thereafter, however, only a ball with a number consecutive (up or down) with that of a ball already removed can be next. In how many different sequential orders (permutations of the numbers from 1 to 15) can all fifteen balls be removed from the table? (Note: If the first ball to go was No. 1, then the sequence *must* be l,2,3,4,5,...14,l5. But if the first ball to go was No. 8, then the next could be 7 or 9; and if 7 went second, then the next must be either 6 or 9; etc.)

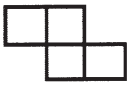
3. In a certain gambling game, a *perfect coin* is tossed repeatedly, until the first occurrence of *tails*, at which point the game ends. What is the expected number of tosses per game? (A *perfect coin* has *heads* and *tails* as equally likely outcomes on each toss, and no memory from one toss to the next.)

4.



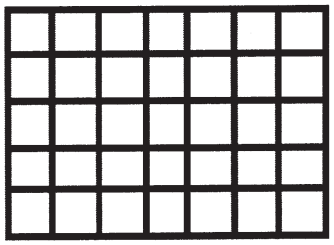
Three identical unit squares are adjacent, as shown in the figure. The diagonals AC, AD, and AE have been drawn in, generating the angles α, β, and γ, respectively, with the line EB. Prove, by elementary methods (no resort to trigonometry!) that the angle α equals (in measurement) the sum of the angles β and γ.

5. When Farmer Brown loaded 1000 pounds of watermelons onto his wagon, they were 99% water (by weight). After a long, hot journey, when he arrived at the market, his watermelons were only 98% water. At this point, how much did his watermelons now weigh? (Assume that the only change was loss of water by evaporation.)

6. Two-sided tiles are available in two shapes:  and  .

a.Using as many as you want of these two shapes, is it possible to tile the 5x7 rectangle?

b. What about tiling a 5x9 rectangle with these two shapes?



Electronic Submission of Manuscripts to the IEEE Transactions on Information Theory

INFORMATION FOR AUTHORS

Overview:

The *IEEE Transactions on Information Theory* will now be supporting electronic submission of manuscripts. The electronic submission is optional, and is intended to expedite the review process.

Submission Procedure:

The author(s) should submit two e-mails to the Editor-in-Chief, one containing a cover letter and the other containing the postscript file of the paper. Alternatively, postscript files may be submitted via FTP (see below). All e-mails should be addressed to:

submit@ece.ucsd.edu

The cover letter must be submitted by e-mail. It should be phrased in the same way as it would be normally phrased for

conventional hard copy submission. In addition, this letter must contain the following information items:

- Title and abstract of the paper. The abstract may be appended at the end of the cover letter, as plain text. Do *not* send the abstract as an attachment. In case the abstract contains mathematical expressions, LaTeX notation may be used.
- Information about the postscript file of the paper indicating whether it is submitted by e-mail or via FTP, including the file name (for FTP submission) or the subject line of the corresponding e-mail (for e-mail submission).
- Name, address, phone number, fax number, and e-mail address of all the authors.
- Manuscript type designation (regular paper or correspondence).
- Associate Editorial area suggested by the author(s).

Author submitting e-mail that contains the cover letter will be automatically assigned as the corresponding author for the paper.

The postscript file of the manuscript should be submitted in one of the following two ways. It may be sent by e-mail as plain unencoded ASCII text. The postscript file should be included in the body of the e-mail. Do *not* send it as an "attached" document. The subject line of the e-mail should be composed of the last name of the corresponding author, followed by the "ps" suffix. (For example, a subject line consisting of shannon.ps would be a valid one.) Alternatively, the postscript file may be submitted via FTP (Internet File Transfer Protocol). To do so, authors should access the following FTP site:

ieee-it.ucsd.edu

login as "anonymous" using e-mail address as password, and put the postscript file in the it_submit directory. The file name should be composed of the last name of the corresponding author followed by the "ps" suffix (e.g., shannon.ps). More detailed instructions for the FTP submission procedure may be obtained by sending e-mail to the following address: help@it.csl.uiuc.edu.

Copyright:

Electronic submission implies a transfer of copyright to the IEEE in accordance with IEEE copyright agreement. If a submission is accepted for publication, a written and signed copyright form would have to be provided by the corresponding author.

Review Procedures:

Manuscripts submitted in electronic form will be reviewed according to the usual editorial procedures and standards of the *IEEE Transactions on Information Theory*. However, the intent is to have all communication between authors, editors, and referees by e-mail, thereby expediting the review process.

Hard Copies:

Hard copies of papers submitted in electronic form ordinarily will not be required. However, the authors should be ready to provide such hard copies at all stages of the editorial review process, upon request from the Editor-in-Chief or from the Associate Editor assigned to the paper. In addition, if and when a paper is accepted for publication, two

SYMPOSIUM REPORT

20th International Symposium on Information Theory in the Benelux Conference Centre "Bremberg", Haasrode, Belgium

May 27 and 28, 1999

The annual symposium of the Benelux Working Group for Information and Communication Theory was this time organized by Prof. A. Barbe, Prof. E.C. van der Meulen and Dr. P. Vanroose of the "Katholieke Universiteit (KU) Leuven", Belgium. The venue of the symposium was in the conference centre "Bremberg", just outside Haasrode in a beautiful landscape setting with good weather and was certainly inspiring to meet other researchers and scientists in the field of digital coding, communication and information theory. About 50 people attended this symposium, mostly from the Benelux itself, some guests appeared from eastern Europe. In total, 29 papers were presented, requiring an afternoon parallel session. Main topics of the seven sessions were compression and video coding, cryptography, speech processing and communication networks, classification and estimation theory, Shannon theory and signal processing and finally, channel coding.

The first session covered a number of presentations on the Context Tree Weighting coding system and an application for language modelling. The second half of the session focussed on image coding with vector quantization, non-static texture coding and embedded video compression for TV systems. In both Cryptography sessions, a number of papers dealt with the timestamping problem, improvements on various crypto schemes, and the second session concluded with a presentation on electronic payment. The speech coding session involved two papers on quality improvement by either noise reduction or subjective quality testing. The last paper presented a scheme for a special coder for GSM telephones, in which the combination

of the speech coder and the employed channel code depends on the quality of the channel. This system was also demonstrated with a prototype. The session on estimation contained papers on linear feature transformations, neural networks and colour pattern recognition. The session on Shannon theory dealt with papers on random parameter channels, feedback channels, duality of source and channel coding, AR coefficient optimization and resource management for adaptive modelling. The last session on channel coding concentrated on more practical issues, such as multirate codes, the BMC channel without feedback, concatenated channel coding schemes and coding for random-access channels. For more details, the symposium proceedings are available in a nice booklet, ISBN 90-71048-14-4, which can be obtained at the Technical University of Delft (NL), Information Theory Department.

On Friday morning, the symposium was enhanced by an invited lecture of Fritz von Haeseler, KU Leuven, Belgium, and University Bremen, Germany, about automatic sequences. On Thursday evening, the banquet was held in a pleasant atmosphere and most of the participants enjoyed the high quality of the kitchen and its wine cellar. As a pleasant surprise, Sergio Verdu, second Vice President IEEE Information Theory Society, attended the dinner. For the second time, the Gauss Foundation kindly supported its paper prize for the best young researchers presentation. The prize was shared this time by two winners: Bert DeKnuydt, KU Leuven, on "Efficient coding of non-static texture in 3D scenes" and Jean Cardinal, Brussels Free University, with a paper entitled "A fast full search equivalent for mean-shape-gain vector quantizers". The annual plenary meeting of WIC members was efficiently supervised so that all could enjoy the combination of Belgian summer sun and traditonal beer.

Peter de With Mannheim,
July 12, 1999.

Successful 1999 IEEE IT-Workshop In Kruger National Park, South Africa

Report by: Han Vinck

One of the twin IEEE 1999 Information Theory Workshops took place from June 20-25, in the beautiful surroundings of the Kruger National Park, South Africa. The organizers of the workshop succeeded in creating ideal circumstances for an inspiring workshop with the general theme: "Information theory and Communications". The workshop was chaired by Hendrik Ferreira from the Rand Afrikaanse Universiteit, Johannesburg, and Shu Lin from the University of Hawaii at Manoa. The technical program chairman was Han Vinck, and the local arrangements were taken care of by Walter Pentzhorn, Martie Branders and Francis Swarts. Although the Kruger Park is in an isolated area, the organizers provided excellent facilities for the 110 workshop participants and their 70 spouses. This number of participants was far above any expectations. The workshop offered many possibilities for game drives in the early morning (06.00!) or in the afternoon after the sessions. Many results on spotting exotic animals like lions, hyenas, leopards, elephants, etc. were reported by the participants. On Wednesday all participants could participate in the tour through the park or in the tour to the environment of the park. The excursion concluded with a traditional "Braai" where as a dessert the whole kitchen staff gave a superb performance in classical South African singing. The technical program consisted of the following sessions: Modeling and Performance Analysis of High Speed Networks, chaired by Tony Ephremides; Multiuser Communication, chaired by Sergio Verdu and David Tse; Coding and Modulation for Fading Channels, chaired by Ezio Biglieri; Spread-Spectrum Communication, chaired by Michael Pursley; Cryptology and Information Security, chaired by Henk van Tilborg; Source Coding Theory and Techniques, chaired by Frans Willems; Identification, chaired by Te Sun Han and Rudi Ahlswede. The recent result session was organized by Mario Blaum and contained 40 papers in three parallel sessions. The timing for the game drives and the sessions allowed many participants to enjoy both of them and resulted in a high attendance during all the sessions. As a highlight in the program, one evening session was organized with two plenary speakers: "Deepening Connections between Coding and Cryptography" by Jim Massey and "An Information Spectrum Approach to Information Theory" by Te Sun Han. The proceedings (131 pages) contains a summary of most of the papers and has IEEE Catalog number 99EX253. In conclusion, the Kruger Park showed to be an ideal place for the workshop which was very well organized by the local community.

WORKSHOP REPORT

The Sixth Canadian Workshop on Information Theory

Kingston, Ontario
June 15 - June 18, 1999

The Sixth Canadian Workshop on Information Theory was held June 15-18, 1999, at The Holiday Inn in Kingston, Ontario. The workshop was sponsored by the Canadian Society for Information Theory, with generous financial support from Communications and Information Technology Ontario, Communications Research Center, the Department of Electrical and Computer Engineering and the Department of Mathematics and Statistics at Queen's University, the Kingston Chapter of the IEEE and Nortel Networks.

The Canadian Society for Information Theory was formed in 1983, following a very successful IEEE International Symposium on Information Theory held in St. Jovite. The purpose of the Society is to promote research in Information Theory in Canada, and this workshop (which is held biannually) is the major avenue by which this purpose is accomplished. Previous workshops were held in St. Jovite, Sydney (B.C.), Rockland, Ville du Lac Delage, and Toronto.

The workshop, which featured 80 attendees from 11 countries, was organized as a single track held over two-and-a- half days. The technical program included five invited plenary lectures and 32 presentations distributed over five sessions. A brief list of the plenary speakers and the sessions follows.

From left to right: F. Alajaji, N. C. Beaulieu, I. Blake, F. Kschischang and G. Brassard.

From left to right: N. C. Beaulieu, L.L. Campbell, F. Alajaji and P. J. McLane.

T. Berger

- *Plenary Lectures*
  (Chair: L. Lorne Campbell - Queen's University)
  - Designing Codes for the Wireless Channel
    Ezio Biglieri - Politecnico di Torino
  - A Conceptualization of Intra-Organism Information Theory
    Toby Berger - Cornell University
  - Performance of Convolutional and Turbo Codes with Quantized Measurements
    Peter J. McLane - Queen's University
  - On Cellular Mobile Communications
    Jon W. Mark - University of Waterloo
  - Quantum Information Processing
    Gilles Brassard - Universit6 demontr6al
- *Channel Coding*
  (Chair: Frank Kschischang - University of Toronto)
- *Source Coding*
  (Chair: Nam Phamdo - SUNY at Stony Brook)
- *Communication Systems and Components*
  (Chair: Amir K. Khandani - University of Waterloo)
- *Wireless Communications*
  (Chair: Jean-Yves Chouinard - University of Ottawa)
- *Information Processing*
  (Chair: Glen K. Takahara - Queen's University)

On June 17, the annual meeting of the Canadian Society for Information Theory was held. During the workshop banquet the *1999 Canadian Award in Telecommunications* was presented to Ian Blake for "significant research contributions, scholarship, and leadership in the fields of algebraic coding theory and cryptography." Previous winners of this award are J. F. Hayes (1996), L. L. Campbell (1994), S. Haykin (1992) and R. de Buda (1990).

E. Biglieri.

The workshop Co-Chairs were Fady Alajaji (Queen's University) and Norman C. Beaulieu (Queen's University). The Technical Program Committee consisted of Fady Alajaji (Queen's University), Norman C. Beaulieu (Queen's University), L. Lorne Campbell (Queen's University), Tamds Linder (Queen's University), Nam Phamdo (SUNY at Stony Brook) and Glen K. Takahara (Queen's University) .

A full list of the papers and contributors can be found at:

http://markov.mast.queensu.ca/~fady/CWIT99/cwit99.html.

The proceedings (ISBN 0-88911-842-6, 154 pages) can be obtained by contacting Fady Alajaji at fady@polya.mast.queensu.ca.

New Books

Raymond Yeung

The Mobile Communications Handbook, 2nd Ed.,
Edited by J. D. Gibson. Springer-Verlag, 1999, 600 pp., $161, ISBN 3-540-64836-4.
Contents: Basic Principles: Complex Envelope Representations for Modulated Signals; Sampling; Pulse Code Modulation; Baseband Signaling and Pulse Shaping; Equalization; Line Coding; Echo Cancellation; Pseudonoise Sequences; Optimum Receivers; Forward Error Correcting Coding; Spread Spectrum; Diversity Techniques; Digital Communications System Performance; Standards Setting Bodies. Wireless: Overview; Modulation Methods; Access Methods; Fading Channels; Statistical Distributions of the Fading Channel; Space-Time Processing; Location Strategies for Personal Communications Services; Analysis of IS-41 C Authentication Protocols for PCs; Cell Design Principles; Microcellular Radio Communications; Fixed and Dynamic Channel Assignment; Radio Location Techniques; Power Control; Enhancements in Second Generation Systems; Pan-European Cellular Standard; IS-54 North American Cellular Standard; British Cordless Telephone Standard; RACE Programs; Half-Rate Standards; Wireless Video Standards; Fixed and Dynamic Channel Assignment; Wireless LANs; Wireless Data; Wireless ATM; Wireless ATM2; Third Generation Systems.

Perspective in Spread Spectrum,
by Amer A. Hassan, John E. Hershey and Gary J. Saulnier. Kluwer, 1999, 176 pp., L59.95, ISBN 0-7923-8265-X.
Contents: Spreading Sequence Design; OFDM Spread Spectrum Communications; Generalization of Walsh Functions; Frequency-Hopped SS with Follower Jamming; Spat)1al Optical CDMA; Spread Spectrum Overlay and Ranging; Appendix A: The Channel's Wideband Effects.

Independent Component Analysis: Theory and Applications,
by Te-Won Lee. Kluwer, 1998, 240 pp., C80.25, ISBN 0-7923-8261-7.
Contents: Introduction; Part I: Theory: Basics, Independent Component Analysis, A Unifying Information-Theoretic Framework for ICA, Blind Sep aration of Time-Delayed and Convolved Sources, ICA Using Overcomplete Representations, First Steps towards Nonlinear ICA; Part II: Applications: Biomedical Applications of ICA; ICA for Feature Extraction; Unsupervised Classification with ICA Mixture Models; Conclusions and Future Research.

Introduction to Matrix Analytic Methods in Stochastic Modeling,
by G. Latouche and V. Ramaswami. SIAM, 1999, 334 pp., $29.95, ISBN 0-89871-425-7.

Remote Sensing Digital Image Analysis: An Introduction, 3rd Ed.,
by J. A. Richards and X. Jia. Springer-Verlag, 1999, 356 pp., $93, ISBN 3-540-64860-7.

High Quality Messaging and Electronic Commerce,
by G. Schmied. Springer-Verlag, 1999, 184 pp., $86, ISBN 3-54064618-3.

Statistical Distributions in Engineering,
by Karl V. Bury. Cambridge University Press, 1999, 328 pp., L20.95, ISBN 0-521-63506-3.

Applied Neural Networks for Signal Processing,
by FA-Long Luo. Cambridge University Press, 1997, 381 pp., L50, ISBN 0-521-56391-7.

Broadband Access Networks,
Edited by Leif Aarthun Ims. Kluwer, 1998, 400 pp., E89.95, ISBN 0-412-82820-0.

Broadband Communications,
by Paul Kuhn and Roya Ulrich. Kluwer, 1998, 624 pp., L 114.95, ISBN 0-412-84410-9.

Communication Protocol Specification and Verification,
by Richard Lai and Ajin Jirachiefpattana. Kluwer, 1998, 328 pp., Z95.25, ISBN 0-7923-8284-6.

GSM: Evolution Towards 3rd Generation Systems,
Edited by Zoran Zvonar, Peter Jung and Karl Kammerlander. Kluwer, 1999, 372 pp., L72, ISBN 0-7923-8351-6.

High Performance Networks for Multimedia Applications,
Edited by Andre Danthine, Otto Spaniol, Wolfgang Effelsberg and Domenico Ferrari. Kluwer, 1998, 204 pp., L72, ISBN 0-7923-8274-9.

Performance and Management of Complex Communication Networks,
Edited by T. Hasegawa, H. Takagi and Y. Takahashi. Kluwer, 1998, 400 pp., L89.95, ISBN 0-412-84250-5.

Performance and Information and Communication Systems,
Edited by Ulf Korner and Arne Nilsson. Kluwer, 1998, 344 pp., L94.95, ISBN 0-412-83730-7.

Dynamic Neural Field Theory for Motion Perception,
by Marin A. Giese. Kluwer, 1998, 288 pp., 09, ISBN 0-7923-8300-1.

Recent Developments in Time-Frequency Analysis,
Edited by Leon Cohen and Patrick Loughlin. Kluwer, 1998, 144 pp., P-72, ISBN 0-7923-8314-1.

Signal Recovery Techniques for Image and Video Compression and Transmission,
Edited by Aggelos Katsaggelos and Nick Galatsonos. Kluwer, 1998, 320 pp., L78.20, ISBN 0-7923-8298-6.

Bifurcation and Chaos in Engineering,
by Y. Chen and A. Y. T. Leung. Springer-Verlag, 1998, 452 pp., $126, ISBN 3-540-76242-6.

Comprehensive Dictionary of Electrical Engineering,
by P. Laplante. Springer-Verlag, 1998, 1540 pp., K58, ISBN 3-54064835-6.

Data and Telecommunications Dictionary,
by J. K. Petersen. Springer-Verlag, 1999, 770 pp., $82, ISBN 0-84939591-T

The Image Processing Handbook, 3rd Ed.,
by J. C. Russ. Springer-Verlag, 1998, 490 pp., $132, ISBN 3-54064747-3.

CONFERENCE ANNOUNCEMENT

3rd ITG Conference Source and Channel Coding

January 17-19, 2000
in Munich, Germany

cosponsored by Informationstechnische Gesellschaft im VDE (ITG), IEEE, Munich University of Technology

The conference will cover the following topics:

- Information Theory
- Source Coding
- Compression for Data, Speech, Audio, Image and TV
- Channel Coding
- Joint Source and Channel Coding, Error Concealment
- Baseband Coding, Multiplexing (e.g., CDMA) and Coded Modulation (e.g., TCM)
- Synchronization
- Cryptography
- Applications

The sessions will start with invited talks by internationally recognized experts. Invited talks will be given by

Prof. D. Costello, University of Notre Dame, USA

Prof. A. Ephremides, University of Maryland, USA

Prof. Th. Ericson, Linkoping University, Sweden

Prof. N. Farvardin, University of Maryland, USA

Prof. D. Forney, Motorola, USA

Prof. R. Johannesson, Lund University, Sweden

Prof. B. Rimoldi, Ecole Polytechnique Federale de Lausanne

Prof. F. Willems, Eindhoven University, Netherlands

For further information please contact the technical program chair

Prof. Dr. Joachim Hagenauer
Institute for Communications Engineering
Technische Universitaet Muenchen
D-80290 Muenchen
Germany

More information is available at

http://www.LNT.ei.tum.de/itg/itg_main.html

CALL FOR PAPERS

Seventh International Workshop on Algebraic and Combinatorial Coding Theory ACCT'2000

Organized by: Institute of Mathematics and Informatics Bulgarian Academy of Sciences
Institute for Information Transmission Problems Russian Academy of Sciences

Time: June 18 - 24, 2000

Place: Blagoevgrad, Bulgaria.

Blagoevgrad is located in the Southwestern part of Bulgaria in one of its most beautiful parts - the Pirin mountain and the Rila mountain. As a university town, Blagoevgrad offers excellent accomodation and conference facilities. There are good bus and train connections with the Sofia airport (90 km).

Topics:

- Linear codes
- Burst-correcting codes
- Self-dual codes
- Algebraic-geometric codes
- Decoding
- Combinatorial codes
- Covering problems
- Computer systems in coding theory
- Related topics

Organizing Committee:

L. Bassalygo (Moscow, Co-Chairman)
S. Dodunekov (Sofia, Co-Chairman)
B. Kudryashov (St. Petersburg)
I. Landjev (Sofia)
S. Kapralov (Gabrovo)
V. Sidorenko (Moscow)
V. Zyablov (Moscow)
V. Zyapkov (Shoumen)

Programme Committee:

N. Manev (Sofia, Co-Chairman)
V. Zinoviev (Moscow, Co-Chairman)
P. Boyvalenkov (Sofia)
V. Levenshtein (Moscow)
M. Tsfasman (Moscow)
V. Yorgov (Shoumen)

Registration fee: US$ 400 prior to March 31, 2000,
US$ 450 after March 31, 2000.
Includes hotel, full board, social events, workshop proceedings.
US$ 250 for spouses.

Submissions: Authors are invited to submit six pages camera-ready papers in English, LaTeX format 11x17 cm by e-mail to: acet@moi.math.bas.bg

Deadlines: January 31, 2000: To inform the Organizing Committee if you are able to come;
March 31, 2000: Deadline for submission (papers to be received);
April 30, 2000: Notification of acceptance (to be mailed out).

Travel information: Will be send upon request by the Organizing Committee.

Inquiries on other matters related to the workshop should be addressed to:

S. M. Dodunekov
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
8 G. Bonchev Str.
1113 Sofia, BULGARIA
e-mail: stedo@moi.math.bas.bg

CALL FOR PAPERS

The 2000 IEEE International Symposium on Information Theory will be held at the Conference Center of the Sorrento Palace Hotel, Sorrento, Italy, from Sunday, June 25, through Friday, June 30, 2000.

Papers presenting contributions to the following areas are solicited:

- Coded modulation
- Coding theory and practice
- Communication complexity
- Communication systems
- Cryptology
- Data compression
- Data networks
- Detection and estimation
- History of information theory
- Multiuser detection
- Multiuser information theory
- Pattern recognition and learning
- Quantum information processing
- Shannon theory
- Signal processing
- Source coding

Papers will be reviewed on the basis of an extended summary of sufficient detail to permit reasonable evaluation. The deadline for submission is **September 15, 1999**, with notification of decision by February 1, 2000. In view of the large number of submissions expected, multiple submissions by the same author will receive especially stringent scrutiny. Abstracts of the papers presented at the Symposium will appear in the Proceedings. Four copies of extended summaries should be mailed to the program co-chair:

Professor Thomas Ericson
Linköpings Universitet
ISY, Datatransmission
SE-581 83 Linköping (Sweden)

It is expected that a small number of grants for the partial reimbursement of travel costs may be available for the authors of accepted papers whose resources would not otherwise enable them to attend the Symposium. Detailed information on the technical program, special events, accommodations, travel arrangements, excursions and applications for travel grants will be posted to the Symposium Web site:

http://www.unisa.it/isit2000

Inquiries on general matters related to the Symposium should be addressed to either of the Co-Chairs:

Professor Ezio Biglieri
Dipartimento di Elettronica
Politecnico di Torino
Corso Duca Degli Abruzzi, 24
I-10129, Torino, Italy
e-mail: biglieri@polito.it
Phone: +39 011 5644030
Fax: +39 011 5644099

Professor Sergio Verdú
Department of Electrical Engineering
Princeton University
Princeton, NJ 08544
USA
e-mail: verdu@princeton.edu
Phone: +1 (609) 258-5315
Fax: +1 (609) 258-3745

GOLOMB'S PUZZLE COLUMN™ PUZZLE NO. 46:

Solutions to "Light Switches"

1. We started with an n x n array of light bulbs, all turned off, and each next to a toggle switch. When any toggle switch is flipped, all bulbs in the row and the column of that switch have their state reversed. (OFF to ON, and ON to OFF). You were asked to find a sequence of switches such that, after they are all flipped, all the bulbs are ON.

The easiest successful sequence to describe is: number the switches from 1 to n^2 (in any way you like!), and then *flip them all* in sequence. Every light bulb is affected by $2n-1$ switches (i.e. all the switches in its row and in its column), so every bulb will have its state reversed $2n-1$ times. Since $2n-1$ is *odd* for all n, and each bulb started in the OFF state, after an odd number of state reversals each bulb will be in the ON state.

2. To the conditions of the previous problem, we added the constraint that a switch can only be flipped if the adjacent light bulb is OFF. It is still possible to go from "all bulbs OFF" to "all bulbs ON", but now the sequence of flips is far more constrained, and the basic strategy we describe depends on whether n is even or odd.

For even n, we can use the following strategy. First, flip each of the n switches, in turn, down the "main diagonal". (After this has been done, the n light bulbs down the main diagonal will be ON, while all the other light bulbs will be OFF.) Next, flip each of the n switches, in turn, down the other diagonal. (Here is where we used "n is even": the two diagonals have no location in common when n is even.) After this has been done, the $2n$ light bulbs on the two diagonals are ON, while all the others are OFF. When $n = 2$, this completes the task. For even $n > 2$, the light bulbs which are OFF can be partitioned into classes of four each, where two light bulbs are in the same class if they are in positions symmetric under successive 90° rotations around the center of n x n array. Since all the diagonal locations have been excluded, no two light bulbs in the same class are in a common row or column. Hence we may pick any one class, and flip each of the four switches of that class in turn, e.g. proceeding clockwise 90° at a time from an arbitrary first member of the class. We then do the same in a second class, then in a third class, and so on until all the switches have been flipped (once each). (We must take care to be sure that each new class, when selected, has its light bulbs in the OFF position.) By the result of the previous problem, all the light bulbs will now be ON. Here are successful sequences of switches for the first few even values of n, following our algorithm.

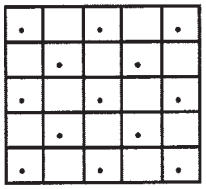
1	3
4	2

1	9	13	5
16	2	6	10
12	7	3	14
8	15	11	4

1	13	21	25	17	7
20	2	29	33	8	14
28	36	3	9	30	22
24	32	10	4	34	26
16	11	35	31	5	18
12	19	27	23	15	6

1	17	25	33	37	29	21	9
24	2	41	49	53	45	10	18
32	48	3	57	61	11	42	26
40	56	64	4	12	58	50	34
36	52	60	13	5	62	54	38
28	44	14	63	59	6	46	30
20	15	47	55	51	43	7	22
16	23	31	39	35	27	19	8

For odd n, we first observe that if there is an allowed sequence of switch flippings that involves precisely the $(n^2+1)/2$ positions on the "dark squares" (including the diagonal squares) of the checkerboard coloring, each location will be state-reversed an odd number of times.

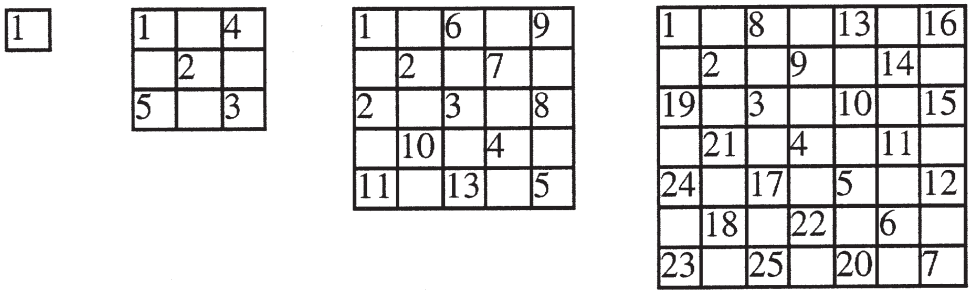
For example, in  if the switches at the 13 dotted squares are flipped, each of the 25 locations will be state-reversed an odd number of times.

The strategy is similar to the even case. We first flip all switches, in turn, down the main diagonal, arriving at the state where the n light bulbs on the main diagonal are ON, while all other light bulbs are OFF. We then flip the switches starting at the third position in the top row, working our way down the "dark" diagonal parallel to the main diagonal. Next we go to the fifth position in the top row (if $n \geq 5$), and proceed down this next dark diagonal parallel to the main

diagonal, and continue in this fashion until all the switches on "dark squares" on and above the main diagonal have been switched. We then go to the dark squares below the main diagonal, flipping each of these switches in turn, subject to the restriction that we can only flip a switch if the total number of flipped switches in its row and column is *even*.

The sequences of recommended switch flippings for the first few odd values of n are shown here.

The ambitious reader may wish to determine which patterns of lit bulbs can be arrived at from an initially OFF *n* x *n*



array, for each value of *n*, or merely what configurations involving the minimum number (> 0) of lit bulbs are achievable, for each *n*.

3. In this problem, you were asked to find a way to determine the one-to-one correspondence between switches a, b, and c in Room X and light bulbs 1, 2, and 3 in Room Y. Here is a solution.

Turn switches a and b to the ON position, leave switch c in the OFF position, and wait a reasonable length of time (e.g. twenty minutes). Then turn OFF switch b, and quickly progress to Room Y. The light bulb that is ON clearly corresponds to switch a. The light bulb that is OFF but *warm* corresponds to switch b. The light bulb that is OFF and *cold* corresponds to switch c. No principles of Information Theory have been violated. Of course, you might ask "How many Information Theorists does it take to change a light bulb?", but that's a totally different question.

Marconi International Fellowship Award. . .

continued from page 5

important role because they were built and sold and worked, which helped build up a reputation for quality and reliability for Codex products. There is a great story that Bob Lucky tells about an Air Force General who visited Bell Labs where they were demonstrating one of their block coding schemes. At the end Bob very proudly stated "and we get a bit-error rate of less than this small number." And the Air Force General snorted: "That's nothing—Codex *never* makes an error … they give you a parity check bit with every information bit."

Bixio: How come low-density parity check codes were forgotten for so many years?

Jim: It was a case of the computing power at the time. Bob Gallager had showed that for a few decoding iterations one would get independent decisions and guessed that the decisions would improve with further iterations. But it was beyond the capability of computers at that time to check this out with simulations. By the time computers got fast enough to do that, people had sort of forgotten about both threshold decodable codes and more specifically about low-density parity check codes. It was only with the discovery of turbo coding that people went back and said "Well, what if we iterate this scheme of Gallager's?" and found out that it is really good. Funnily enough, it turned out that if you iterate the threshold decoding of what I called convolutional self-orthogonal codes they also perform well. Not as well as turbo codes but surprisingly close to the capacity of the channel.

Bixio: Given that there was a company founded to implement your threshold decoding and given that people thought that all problems in information theory were solved, did you ever think of joining Codex instead of going back to Notre Dame as a faculty member?

Jim: No, I still had the missionary attitude that it was my responsibility to go back. I guess that my Catholic schooling had left me a strong sense of duty, that one lives not only for himself but that what you did for your fellow man was more important. I never had the notion that I should be a great researcher or that I should try to maximize my own potential as a researcher. Maybe that was a good thing, maybe a bad thing. I don't know what kind of researcher I would have been if I had tried to maximize my research contributions, but it would not have been me.

Bixio: It must have been particularly hard leaving MIT for Notre Dame where, in those days, you were alone working in information theory.

Jim: I regretted leaving doctoral studies at MIT, but this doesn't mean I wanted to stay on as an assistant professor at MIT as many people did in those days. There was some kind of Ford Foundation plan to support this. The doctoral time is

a wonderful time. One is free to do what he wants, even to go to the library and read papers. It is really a nice time and I think I could have profited from more of that. It is true that all through my fifteen years at Notre Dame I was alone in information theory. But I don't think that this was a disadvantage. What it meant was that to interact with my colleagues I had to learn something about control, about automata theory, and other things that if I was too narrowly working on information theory I might not have been tempted to pursue.

I always tell my doctoral students that if a problem is interesting there is a doctoral dissertation in it. I never have felt the need to have a lot of colleagues around working on very similar things. In fact I am always a little suspicious of people who tell me, "I don't want to stay here because there are not enough people working in my area to interact with." I always think "Wait a minute …can't you think for yourself?" There comes a time when we should be adults in the field and not need somebody else to guide us and to tell us what to do. I think that when you become a faculty member that time should have arrived.

At Notre Dame, I was involved in everything. I was well known on the campus from having been one of twins who were the top two students in their class. All the professors knew me, and Jerry and I were very good friends with Father Hesburgh who was the president of Notre Dame. I was also involved with every administrative thing that came along. During the student uproar of the late sixties, I chaired a committee made up of faculty, students, and administrators, which was a kind of committee of last resort for handling students' problems. Such things took a tremendous amount of time out of my technical work but they also had their own values, their own meaning and I learned from them also. I can't say that I regret it.

Bixio: Tell us about the teacher who knows how to motivate students and knows how to find simple ways to explain difficult subjects without compromising rigor.

Jim: That's a tough question for me. I already mentioned Vladimir Seidel to whom I am indebted for teaching me the spirit of mathematics. I think that most people would say that he was a lousy teacher but he was exactly right for me because he gave proofs that were completely rigorous and as simple as they could be, which I think is what you want to do. I also learned something useful from him about teaching. He always came in and would write the theorems and proofs impeccably on the blackboard, but he never used notes. That impressed me as a student and I thought that if I ever became a teacher I was going to do that, too. There is nothing worse than going to a class where the teacher takes out old yellow notes and starts copying things onto the blackboard. Seidel never did this. The only time he would ever use notes was when he gave us an exercise. Then he might take a matchbook out of his pocket, open it up, and on the inside cover of the matchbook would be a problem that he would then write on the board. I have stolen from other teachers techniques that I thought were good and motivating. I have also heeded advice sometimes. Like when I was giving a talk on threshold decoding at MIT, Jack Wozencraft chided me for writing all over the board instead of systematically going from left to right and keeping things in nice order. He was right, it makes a big difference.

Bixio: Let us now talk about research. Your wide spectrum of research includes coding theory, multiple access, and cryptography. It looks like rather than switching from one topic to another, from time to time you would add a new topic to the list. How did this happen?

Jim: New topics came because something caught my interest and I said "Hey, that's neat" or "I ought to learn about that because that sounds like it could be fun." It was that way, for example, in random-access communications, in multi-user communications, in cryptography, in the mobile radio aspects that I have worked on, and in the design of sequences. It has always been because something caught my attention, never because I thought it was important.

Bixio: Can you give us an example?

Jim: I think in cryptography it was the Diffie-Hellman work that suddenly made this area exciting. It was a new idea and it piqued my interest to go into that area.

Bixio: How much time do you devote to reading the literature?

Jim: Almost none. Usually when I receive the Information Theory Transactions I will glance through the titles. Occasionally I see one that interests me and I read the abstract. Almost never do I read the paper. The only papers I really read are the ones that I review. That's very useful because then you do have to sit down and check things out. It is a good intellectual exercise.

Bixio: Has it always been that way?

Jim: I'd say yes since my doctoral student days. There you had more time and you occasionally went to the library. One of the advantages in those days was that there wasn't ready access to copy machines. I remember it cost 25 cents a sheet to make a thermofax copy at that time. If you are getting $250 a month, 25 cents for one sheet is a lot of money. So you were very careful if you actually were going to copy things. The result was that you would go to the library, read the paper, and make little notes of what you should remember of the paper. This was a lot better than having a copy of the paper sitting in your desk drawer. Maybe we should encourage our students to do something like this … perhaps raise the price of copies.

Bixio: How did you get your best ideas?

Jim: They came at strange times. For example I remember the idea of the collision channel without feedback came when I was taking a nap. Just before going to sleep the idea popped into my head. The key proof that I needed in the shift register synthesis algorithm came to me when I was out on a walk and not thinking about the thing at all. Suddenly it popped into my head … that's how you prove it! It seems

that your brain continues to work on problems even when you are not consciously working on them.

Bixio: What research contribution are you most proud of?

Jim: I think most researchers are always most proud of their last contribution. I just recently did something on what I call optimum transform diffusion; it has something to do with cryptography. I think it is kind of neat. But there is nothing that really stands out, something that I am particularly proud of. Certainly the thing that has given me the most mileage has been the so-called Berlekamp-Massey algorithm because it has been used so widely and referred to so often.

There have been a few times in my life when I really got excited intellectually about something. One of those was in developing the shift register synthesis algorithm, a version of Elwyn [Berlekamp]'s BCH decoding algorithm that solved the problem of finding the shortest linear feedback shift register to generate a sequence. I remember being really intellectually excited about that. Another time was the work I did on generalized Reed-Muller codes, which has gone virtually unnoticed but it excited me at the time. Another time was when it suddenly popped into my head how to communicate over the collision channel without feedback. So there have been a few times when I got really excited about something. Sometimes I have gotten excited and it's not panned out at all. But those three times I remember. I can't say that in retrospect those results were worth a lot more than others.

I always tell people "Look, a hundred years from now if our name appears in a book on information theory in a footnote, we will be lucky." What we do is all relatively minor if you compare it to the work that Shannon did, founding the field, starting it all. I don't see any reason to get filled with pride about adding an epsilon to something, which is what we mostly do. Maybe we can get two epsilons if we are lucky. But we don't get much farther than that.

Bixio: I have never seen you doing anything you were not excited about.

Jim: I think that having fun and being intellectually excited are two different things. I am always doing it because I like to do it, yes. And that creates a certain kind of excitement but I don't often deceive myself by thinking "What I am doing is really important and I have just made a great contribution."

Bixio: Let's talk about your industrial contributions. Some of your codes have become a standard for NASA. You have several inventions that played a key role in ESA's [European Space Agency] missions. You have also designed IDEA [International Data Encryption Standard] which has been incorporated into the PGP [Pretty Good Privacy] software package available and widely used on the interned. Tell us about these inventions and how it feels to see your ideas being so widely used.

Jim: Let me start with the standardized NASA codes. These were the codes that Dan Costello and I developed together: the quick look-in codes for space communications. They got used in a lot of deep-space systems for a number of years and I think some systems still use them. That was always nice to hear about but I never followed those things. I never paid attention to what flights were using our codes. Once I had done the work it wasn't of interest to me anymore. I knew it was going to work. Same way with the IDEA cipher that I developed with Xuejia Lai, who did most of the work on it. Once it is there I lose interest in knowing who is using it. First of all it is very hard to find out such information and if you really start searching you end up with an enormous amount of correspondence with people. I just never paid attention to those things. I accidentally hear from time to time that PGP is using IDEA, or somebody else is using IDEA, but I have never made an attempt to find out.

Bixio: Tell us about Cylink, which is your second start-up company and is a leading supplier of data encryption products.

Jim: Again it is another fluke. Cylink came about because Jim Omura and I were doing a short course that we called Principles of Secure Communications. Security meant two things, security against noise and also security against a cryptanalytic attacker. We had broken the course down so that Jim did the spread-spectrum part and I did the algebraic coding and cryptographic aspects. We always went to each other's talks to keep the course unified. Jim started getting more and more interested in cryptography and we ended up making a couple of small inventions and filing patents on those. Jim was absolutely determined to set up a start-up company to develop these ideas. And he did, with the help of other people like Lew Morris, who was the first president. They set up the company and again I was given some stock in exchange for patent rights. I have been associated with the company ever since.

But you have to give 99 percent of the credit to Jim and 1 percent to me because it was Jim who actually resigned as a professor at UCLA and devoted himself full time to building up the company and making it into a success. Just recently the company has run into hard times and I hope it is going to come out of those soon, but we will have to wait to see what happens.

Bixio: Has it been financially rewarding to create two startup companies?

Jim: Wait a minute. You mean: "having a small role in the creation of two startup companies." Yes, I made quite a bit of money out of Codex and I have already made quite a bit of money out of Cylink. Because of that we can live pretty comfortably in retirement.

Bixio: Tell us about your free time.

Jim: That's difficult. You know that I have a charming wife, Lis, and it is because of her that we live in Copenhagen now. She is Danish. This way we are able to be close to seven of our thirteen grandchildren and my life revolves around the family and our dog, Oliver. Oliver takes a good deal of attention from me since we make four relatively long walks a day around Copenhagen. I like to read when I get a chance. I have

no musical talent whatsoever but I like to listen to good music. I don't have any real hobbies, but I do like to work around the house and repair things. At the moment I am into clocks. I have been repairing clocks in our house. We have a lot of old clocks. I am trying to get them all to run as precisely as possible. I like to do electrical and mechanical things in the house, but I am not very good at plumbing … it is too difficult.

Bixio: What about sports?

Jim: I avoid those.

Bixio: You work very hard and you've never felt the need for an outlet?

Jim: In fact I used to play a lot of handball when I was a graduate student at MIT and a student at Notre Dame and I always liked to play golf but it was difficult to find enough time to get to be good at it. It takes a lot of practice to become a reasonably adept golfer and I was never willing to put that in. I liked to play tennis when we lived in California but I was never good at it. I always enjoyed playing sport for the fun of it but I can never understand jogging or exercising, or things of this sort, things that seem to be a punishment to the human body that one should avoid. In Switzerland I liked to ski but I never used to do the preparation before the season and never would exercise to get myself in shape for it. I do walk a lot and I think that is enough exercise.

Bixio: A year ago you retired from ETH. Do you have any big plans for the future?

Jim: No, but I do hope to write a beginners' book on information theory. If everything works out well I might at some point attempt to write a book on cryptography. I have some big problems I'd like to work on, a couple of key problems I have been interested in. On the cryptographic side I think the problem with the greatest intellectual need to be solved is the following: is there such a thing as a one-way function for a "reasonable" definition of difficulty? Right now we know nothing about this question. This interests me, but not because it is important. Cryptography is doing well enough without an answer to that question, but intellectually it bothers me that we don't know whether these things really exist or not. We go out and say "here is a one-way function so let's use it", but we don't even know if a one-way function exists. It is not like in coding theory where you knew that good codes existed but you couldn't find them.

Bixio: What made you decide to take early retirement?

Jim: I was getting too bogged down. I was falling further and further behind with things I should get done. I just wanted to get away from it all, have a little more time to enjoy life and do more of what I wanted to do.

Bixio: Did Lis play a role in this decision?

Jim: Yes. Also, as you know, I had a severe illness a couple of years earlier and that also tipped the scales. It didn't make sense to continue at the pace that I was going, but there was no way I could slow down. It was either retire or continue the same way.

Bixio: Many people wonder why you have never written a textbook.

Jim: It has to do with laziness, Bixio. Laziness is one reason, certainly, but it takes a lot of time to write a good book and I just never have felt I had the time. I hope to do that now that I am retired. But this first year of retirement I have been even busier than before. I just recently finished three doctoral students at the ETH. And I am involved now in a lot of external lecturing and consulting and so on. I even haven't had enough time to unpack all my stuff from my office at the ETH and to set up my home office properly. When I do that I would like to write a book on information theory for beginners. I mean for real beginners, a book aimed at the student, not at the person who already knows information theory.

Bixio: Let us conclude with a few general questions. Eighteen years ago you moved from the United States to Europe. Any regrets?

Jim: No, none whatsoever. We really enjoyed the time in Switzerland. The ETH is a wonderful place to be a professor and I enjoyed it immensely. For Lis it was very, very important … we had just been married for two years when I decided to accept the offer from ETH. She really wanted to get back to Europe to live and that suited me. I think I can be happy anywhere. I can certainly be happy living here in South Africa, I can be happy living in Moscow, I can be happy living in Copenhagen and I can be happy living in virtually any place.

Bixio: The university systems in the U.S. and in Europe are quite different and you know them both very well. If you could take the best of the two worlds how would your university look like?

Jim: This is a good question, Bixio. My knowledge of the American system is a bit outdated because it has been eighteen years since I was there but I feel that in the U.S. system, as I remember it, we indoctrinated the students too much. Students were required to take too many lectures and spend too much time following a kind of curriculum that would be laid down for them. And then they would move directly into a thesis that would be more or less laid down for them also. In Zurich there were no graduate courses whatsoever required for the doctor degree. I think that's healthier. Maybe you might have a happy medium in which you could have certain very basic courses, in mathematics for example or basic systems engineering, or certain areas that have a wide generality but are treated in more depth than they would be in an undergraduate course. The students in the first year might attend some of these lectures. But I definitely think that in the U.S. we overdid the stuffing of packed material into the students.

I also think it is good if the students can interact a lot with their professor. This is better in the U.S. system than in Europe because typically there are more professors per graduate student in the U.S. At the ETH maybe there were about 15 doctoral students per EE professor and it's the rare professor who can keep in close contact with his students, know what

they are doing, help them when they get stuck, or at least encourage them. I think that encouraging is more important than helping. Encourage them, listen to them, and get interested in what they are doing. These are the important things. It would be nice in the European system if we had more professors. Actually I don't think that we need more professors but we need fewer doctoral students. I always thought that we had too many at the ETH. I don't know what all these doctors are going to do when they finish. I think we would have done better with half as many doctoral students and the same faculty that we have currently, but that's probably not a view that is widely shared.

Bixio: But you encountered and fell in love with information theory in one of those "unhealthy" graduate courses.

Jim: You nailed me on that one, Bixio. But Fano was unusual in that he stressed the intuition of the subject, something that few professors do in graduate courses.

Bixio: What are the big lessons that you have learned throughout life?

Jim: Don't trust the experts. Don't believe anybody. Think for yourself. That's the most important one. When I have followed my own instincts, my own beliefs, that's when things have worked out well. I already mentioned the advice I received that coding theory was a bad area to try to do a thesis in. My instinct was no, this is fun, I have to do it. I think in some ways our lives are pretty well prescribed for us. In our work we have more freedom than in most things in life and we should use it.

Bixio: Any advice for those who are concerned about the education of our children?

Jim: Don't worry about it. I think we worry far too much about educating our children, seeing that they get into all the best schools. I noticed this very much at MIT when I was a teaching assistant. All the undergraduates at MIT are smart people. They have all been number one in their class and had top scores on the various examinations. And yet when you get them in the classroom [at MIT] some of them would do very poorly. This is because they have been used to excelling and suddenly they are at the bottom end of the curve instead of being at the top end. This is a great psychological shock for a number of these people. Many of these would have profited from a more democratic intellectual environment where you had a real spectrum of skills. I know for example when we were in our small grade school, the teaching sisters had my brother and me helping other children. That was good for us. If we had been in a school for gifted children I don't know what would have happened to us. I think we worry far too much about education for children. Kids will find their way.

Bixio: A last question: how do you compare the field as you started out and now?

Jim: Well, I think that there are a lot more smart young people. I am really impressed with the quickness and breadth of many of the young people working in the field. I am really pleased about that. Information theory seems to be attracting good people. If there are things I don't like … I think our Transactions are more boring than they used to be. There is a need apparently to publish papers, to get promoted and get tenure. Many more papers are written than should be written. I don't know what one should do about that. If you look at the old Transactions they were pretty interesting. We didn't have the disadvantage of good word processors. Papers had to be typed out and you had to carefully think what you were writing. You couldn't copy a segment out of one paper and stick it into another paper. You even wrote papers by hand for the first couple of drafts which was probably a better way of doing it. We also didn't write so many papers. In fact my publication record I am sure is much less than most of the young people nowadays. We didn't have that pressure on us to publish. I think we were better off for not having that pressure. It has to do with what I think is the cowardice of universities. Universities hesitate to make decisions based on their own knowledge. They have to try somehow when they make a tenure decision to make an objective decision. That means they try to get certain parameters they can measure, like how many papers in refereed journals, letters of reference from the outside, etc. People inside know the quality of the candidate much better than the people outside writing these letters. They should know whether the person is someone who will serve that university well or not. They should themselves decide on these things.

Bixio: Thank you, Jim. It has been a great pleasure interviewing you. I wish you good luck towards proving the existence of one-way functions.

Jim: Thank you, Bixio. It was a pleasure talking with you and I hope I didn't provide too much bad advice for the readers.

Harvey Prize. . .

continued from page 1

where. It was a bright bunch of people, but unfortunately our officers and non-commissioned officers were only marginally literate.

Forney: What was this army unit?

Gallager: It was called a scientific and professional personnel unit. It was the army's effort to make good use of people who had an engineering or scientific background. It was not so much a communication unit as what is now called C^3I. We worked on something called battlefield surveillance. It was not only communication but also networking and control. It is amazing to me that over the last forty years, there has been so little real progress in that field.

Forney: Were there any personalities that particularly affected you in the army?

Gallager: Well, there was a colonel who had very different views on the way things should be done than I did. I remem-

ber that at one point he had all of us out on the field, running around with little slips of paper, which was his idea of how battlefield surveillance would be done. The officers sat in the van and wrote notes, and we peons took the notes and ran from one van to another with them. At one point I wrote to my senator that we weren't being used as scientific professionals. The colonel found out about this and he was very upset, to put it in printable language. He assigned me to stockade guard duty for three months. This was one of the best assignments I ever had, as I had nothing to do and spent the time studying lots of things and thinking through problems. It was a far more academic environment than anything I have experienced since.

Forney: I suppose that is where you first read Claude Shannon?

Gallager: I had heard about Claude Shannon at Bell Labs. In the army, sometimes in the morning I had a terrible hangover and would go to the library for peace and rest. That was where I first started to read Claude Shannon. Before that, I had tried to read about information theory as interpreted by others, and had no idea what they were talking about. When I started reading Shannon's own papers, it all seemed so simple.

Forney: You have consulted for the army subsequently, haven't you?

Gallager: I have been involved in a number of committees trying to help the U.S. Army. The army has always been planning for fifteen years ahead, but never thinking very much about the near future. As a result, soldiers in the field still don't have the kind of personal communication devices that we civilians have.

Forney: How did you happen to go to graduate school at MIT?

Gallager: Well, I was planning to go back to Bell Labs, which I had thoroughly enjoyed. But then I learned that draftees could get out of the army three months early by going back to graduate school. I planned to go to graduate school for one term. If I liked it, I would stay for two terms and get a master's degree. I applied to the EE Department at MIT and to the Math Department at Yale. I got a fellowship offer from each, but MIT started one week earlier than Yale did. Since my main objective was to get out of the army as soon as possible, I went to MIT, which has shaped a great deal of my later life.

Forney: That was fortuitous, because MIT at that time was a very exciting place. How long did it take you to find the information theory group at MIT?

Gallager: I think it took me about two or three weeks. When I first arrived at MIT, I thought I was interested in switching theory. I talked to Dave Huffman, who was the switching guru at that time. After about ten minutes, he essentially told me that all the action was in information theory. Pretty soon I was talking to Bob Fano, who was suggesting all sorts of crazy things to work on. They weren't actually that crazy, but I was expecting something a little more oriented toward applications. Despite myself, I found myself doing research.

Forney: Could you paint a picture of what MIT was like in those days?

Gallager: It was a very exciting environment. It was just a year after Claude Shannon had come to MIT from Bell Labs. Along with Claude, the faculty interested in information theory at the time included Bob Fano, Peter Elias, Dave Huffman, and Bill Youngblood. Jack Wozencraft was finishing his thesis and about to join the faculty, and Bill Davenport soon moved to campus from Lincoln Lab. Jack's work on sequential decoding was very hot in that era, and still has a lot to recommend it. There was another large group doing what was called statistical communication, under Norbert Weiner and Y.-W. Lee. That group tended to be more oriented towards continuous mathematics and control. The information theory group was more oriented towards discrete mathematics, algorithms, and the kinds of the things that information theorists still do. It was very exciting because there were many different currents swirling around. The early days of computer science were taking place in the same building. John McCarthy and Marvin Minsky were there, feeling somewhat frustrated that MIT wasn't paying enough attention to the emerging field of computers. The brightest new graduate students were strongly attracted to Information Theory. The group of students who were there then and shortly after includes many of the best-known people in information theory and related fields today. They included Elwyn Berlekamp, Roger Brockett, Dave Forney, Irwin Jacobs, Fred Jelinek, Tom Kailath, Bob Kahn, Len Kleinrock, Jim Massey, Larry Roberts, Harry Van Trees, Jan Willems, and Jacob Ziv.

Forney: How long did it take you to find a thesis topic?

Gallager: It didn't take very long to find a master's thesis topic. Bob Fano suggested a problem, and it was fun playing with it. I don't even remember what it was any more. In retrospect it wasn't very important, but it was good training in doing research. As I said, I wasn't planning a life in research; I was just intending to go back to Bell Labs. However, after a year I was really hooked on MIT and decided to stay for a Ph.D. It was relatively easy to find a Ph.D. problem in information theory since almost nothing was known. One could

work on almost anything and it would be new. After looking at Pete Elias' iterative coding schemes for error correction, I got the idea that long block lengths were good for achieving small error probability, but that the parity-check equations should be kept simple to avoid decoding complexity. This led me rather quickly to the idea of low-density parity-check codes. However, it took quite a bit of work before I could see how to analyze them.

Forney: Was Bob Fano still your advisor at this point?

Gallager: No, I switched to Pete Elias since he was closer to the ideas that I was pursuing at that time. He was a wonderful thesis advisor, always willing to listen even though he was Chairman of the Department by the time I turned in the thesis. Even after that he was always interested in what I was working on, and seemed able to understand new ideas almost instantaneously.

Forney: Your work on low-density parity-check codes was more or less forgotten for thirty years, but recently has become one of the hottest topics in coding theory. What would you say about that history?

Gallager: Well, actually there were a few people who kept toying with the idea. Some years later Mike Taylor was trying to construct reliable memories out of unreliable components, and it turned out that low-density parity-check codes were a nice way of getting around any type of failure, whether in memory or in computation. Also, after the Russians translated my LDPC monograph, there was a flurry of activity there. I think the reason that interest died out was that other techniques seemed more promising and were closer to the technology of the day. LDPC coding required block lengths so large that even though hardware requirements went up slowly with block length, they were too intensive for those days. Thirty years later, the technology was available. People working on turbo codes recognized that they were very similar to low-density parity-check codes. That's what led to all this new activity.

Forney: How valuable did you think your thesis was at that time?

Gallager: I think that all of us who do theoretical work jump between thinking our work is wonderful and thinking our work is totally useless. I remember an interview at IBM during which I said that I had developed a coding technique which would allow one to transmit at an arbitrarily small error rate at a data rate arbitrarily close to channel capacity. The interviewer was very offended. He thought that this was really bragging and that my technique wouldn't work in practice because it was too complex, and of course at that time he was right. On the other hand I was right too. So while I was happy with what I had done, I also realized that it wasn't something that could be used at that time. As time went on it seemed less likely that it would ever be used, but much later people found that it might in fact be practical. It's sort of the way of many theoretical developments.

When we are honest with ourselves, we have to admit that we don't know whether our work is going to be useful or not. Even if it is useful, there are usually so many other further steps by other people that we can't really say how important our idea was in the whole development.

Forney: What did you work on after your thesis?

Gallager: I worked on a strange channel model in which, along with ordinary errors, the channel could also delete and insert symbols. I applied sequential decoding to this channel model, and proved some nice things about decoding with arbitrarily small error probability. I was quite proud of the resulting paper, and submitted it to the 1962 Symposium on Information Theory in London. I got a polite letter back from Colin Cherry saying that they liked my paper but couldn't accept it because there were too many papers from MIT, and all the other papers were by more senior faculty members.

Forney: Then what?

Gallager: I interviewed at a number of places, including Bell Labs because of my fond memories there. I remember clearly talking to Brockway McMillan, who had done good early work in information theory. He told me what some MIT people were saying in the early 1960's, which was that information theory was sort of dead. McMillan told me that I ought to get into military communications, which is what he was doing at that time. I felt that at some level he was right, because after this tremendous spurt of activity at MIT in information theory, we didn't see much happening, because the technology wasn't ready for the complexity that we were thinking of. At the same time, I was still fascinated with the field and wanted to work in it. So when MIT made me an offer, I decided it was an offer I couldn't refuse and thought I would stay there for a few more years. I was very lucky because whereas most young faculty members feel great pressure about getting tenure, I never did because I was never sure whether I wanted to continue to teach. So one day I just found out I had tenure.

Forney: I know that you were involved in the founding of Codex Corporation in 1962, and I would be very eager to hear your recollections.

Gallager: When I was a graduate student, I consulted for a company called Melpar, which was a Washington firm that did mostly defense work. Its research division was in Boston, and the Director of Research was Arthur Kohlenberg. Arthur was a person who most information theorists at that time knew well and respected highly, a wonderful engineer and scientist and a wonderful person. I enjoyed working there. Jacob Ziv consulted there also for a while. The management at Melpar evidently felt that these researchers up in Boston had too much freedom and eventually decided to bring them back under closer control. Arthur and Jim Cryer, the manager of the Boston division, thought that this might be the time to start their own company. They thought that this coding business could be a hot thing for the future, so they wrote up a business plan and started Codex. I was a consultant. I told them about the threshold decoding work that Jim Massey was doing in his thesis. They decided that this would be a great place to get started, so they asked Jim to consult for them also, bought the rights to his invention, and started developing products. We think that today is an unusual time in which people can start Internet companies and have market values of billions of dollars before they make a single dollar. But this happened in the 1960's also. Codex lost money for a long time, but it went public and the stock went up and up.

I think the most valuable thing I ever did for Codex was to tell you about them and them about you when you were finishing your thesis. I thought that you would probably want to go into an academic environment, but much to my surprise you found this entrepreneurial seat-of-the-pants operation very intriguing and started to work there. That made consulting for Codex even more enjoyable.

Forney: Did you ever consider leaving academia and going to work for Codex?

Gallager: Yes, I thought about it a number of times. For me Codex was sort of a vacation from MIT, where I could sit and think and nobody would bother me. But then I saw that the people who were actually working there were scrambling constantly, and that their lives were just as chaotic as mine was at MIT. So I decided to stay at MIT, and continue consulting at Codex, which was much more fun.

Forney: I can certainly testify that you did a lot of valuable engineering there. And your interests evolved as Codex's interests evolved. In the 60's you were very heavily involved in coding, and developed some burst-error correcting codes for Codex. At the end of the 60's you were the one who got us on the path to QAM modems, which was probably the most valuable thing you did for Codex. Then later your interests evolved into networking. Was this just pure happenstance?

Gallager: Well, I think my change of interest was partly influenced by Codex and partly by other things. In the late 60's, coding ideas had gotten far ahead of what we could build, while the more mundane parts of communication had somewhat languished. So there was wide interest in how you could actually build better communication systems. I got into QAM because Codex had hired Jerry Holsinger, who had some nice ideas for building 9600 b/s modems. That doesn't sound like much now, but it was a lot then. Jerry was doing this with a single-sideband modem, which was what most people were advocating in those days. I started trying to figure out how these things worked and got so frustrated with Hilbert transforms and the like that I said that there must be an easier way. Why not just build a double-sideband modem? It would be much easier, carrier and timing recovery would be much easier, and we could understand what we were doing. So I spent a couple of years trying to flesh that out. Then Codex went through a rather bad period in 1970 where both its two founders died, the military business was doing poorly, and the modem business wasn't going well either. To survive, the company suddenly had to develop a new modem very quickly. Dave Forney took the project over, decided the best bet was the double-sideband approach, and in an amazingly short period of time developed a viable modem product. The company's fortunes were made for quite a long time.

Forney: Probably your most famous paper is your 1965 exponential error bound paper. Is that your favorite paper?

Gallager: That is certainly my favorite paper. However, I've always liked my books more than my papers because what I have always enjoyed doing is taking ideas and trying to make them simpler. I get frustrated by things that are too complicated. The way that work actually began was that shortly after I was hired, MIT decided to teach a double graduate course in information theory and coding. Part of it was to be on sequential decoding, and part was to explain the theoretical development of the coding theorem and so forth. Bob Fano had just published a book on information theory which had a proof of the coding theorem, and I was going to teach this in this class. But I couldn't find a way of presenting that work because there were a number of optimizations, and I couldn't see why they were maxima instead of minima. I had four or five almost sleepless nights trying to figure out how I would present this stuff. Finally it all just came to me in a rush. This was a good example of teaching and research really fitting together well. Many times, trying to understand something well enough to teach it has given me nice new ideas for research.

Forney: Was there more or less a straight line from this to your 1968 book?

Gallager: There was certainly a straight line to the coding theorem part of the book. The other parts of the book took an awful lot of work. That book was probably five or six years in the making. As I went through it I found that many of the things that I thought I understood really weren't very well sorted out anywhere in the literature. All the things that people thought that they knew about the Gaussian channel seemed to become very vague when one tried to present them precisely. I probably wasted about a year of my life trying to do the Gaussian channel precisely. I'm not sure it was worth it because everyone understood what was going on anyway; it was just a matter of crossing the t's and dotting the

i's. I think it was worthwhile, but now when I write papers, I usually say that this is just the way it is.

Forney: Are you ever going to produce a revision of that book?

Gallager: I really don't know. I am currently writing a book on stochastic processes, which is a second edition of an earlier book. I am trying to put in detection and estimation and Gaussian processes and other things. There are some other books and projects that I have in mind. If I ever get those things done, then I will go back to the information theory book and rewrite that.

Forney: We are up to the 1970's. What happened then?

Gallager: Well, networks were starting to become very important at that time. I started focussing on them at MIT, and also it was something that Codex was getting involved in. I first got involved in routing, which is what most academic people first get involved with because it's a very nice analytical optimization problem. Then I got more interested in congestion control, and later in all queuing aspects of networks. After that I got more and more involved in network architecture. Information theory and communication are fields in which theory and practice are probably closer than in any other field of technology that I know of. The network field is probably at the other extreme, where theory and practice have very little to do with each other. The more successful developments are usually totally ad hoc. The Internet protocols were developed by people who thought very well architecturally, but there was almost nothing of an analytical nature in that work. I'm still very curious to see whether we will ever have a networking theory that allows people to understand what's going on in networking in a cleaner way.

Forney: Was it frustrating to try to develop a theory of networking?

Gallager: It was frustrating, but it was also fun. It was fun because nothing was known, so in that sense it was like the early days in information theory. But it was frustrating because one got the sense that no one who built networks really cared. They were going to build networks the way they were going to build networks. In retrospect, I think we are starting to get a better idea of what's going on in networks; the theoretical work that's been done has had some impact, but not nearly as much as one might have hoped.

Forney: Many people have wondered what happened to information theory and communication theory at MIT. What can you say about that?

Gallager: It's a long story. As I said, even in 1960 MIT had started to partly turn away from information theory, and later much more so. In the 1970's, U.S. universities tended to feel that the pendulum had moved too far towards making a science out of engineering. There was a feeling that engineers should go back to being engineers. They should use insight more and mathematics less. They should use simulation and experiments more and should think less. It was a great change, which I believe is still going on. I think that there was good reason for some of these changes. Much of the academic work in engineering had gotten overtheoretical and divorced from real problems. What has been surprising in information theory is that the theory just kept going. Moreover, it kept getting closer to practice, and practitioners somehow managed to make use of the theorems. In part this was due to a number of very good theoretical people who were also very good engineers. Irwin Jacobs is an example of somebody who understands how to build a company very well, but who also understands all of the scientific underpinnings and therefore moves in the right directions.

I think that now we've moved too far in the direction of emphasizing building things, in a broader but shallower kind of learning. People are studying complexity a lot these days. To me, a complex system is a system we don't understand. When even very large systems are well designed, such as the telephone system or today's mobile systems, in some sense they are not complex because they are architected right and they follow simple principles. Even though there are an enormous number of devices, people can understand what they are all doing. To me, complex systems are simply systems that nobody has taken the time to understand. So I think that we should be focussing more on trying to make things simple.

Forney: You've also worked on optical and wireless communication. What is your view of these fields?

Gallager: Optical communication is clearly an important field. However, it doesn't have many nice problems for students to work on. Wireless communication, on the other hand, is a field with an enormous number of very nice communication problems. The fact that the channel has multipath and fading makes it much more interesting than the pure Gaussian noise channel.

Forney: You've produced a great many good graduate students. What are your thoughts on the student-teacher relationship?

Gallager: It's clearly one of the most rewarding and enjoyable parts of being a faculty member. The opportunity to work with first-rate students is wonderful. Sometimes I've found that working with students who don't seem to be quite first-rate is also wonderful in terms of seeing them evolve. Then you feel that you have had an impact on them, whereas the very best students will probably do first-rate research regardless of their advisor. One of my earliest Ph.D, students was Elwyn Berlekamp; I probably didn't contribute much to his thesis since he knew exactly what he wanted to do and how to do it. However, many other students need quite a bit of guidance to do research.

Forney: What are your plans for the next couple of weeks?

Gallager: I will be travelling with two grandchildren and with my wife, Marie. We're going to Israel first for the award

of the Harvey prize. Then we are going to South Africa and Greece for two Information Theory Workshops. After that I think I will spend the rest of the summer recovering, trying to finish my stochastic processes book, and reading some thesis proposals. I have 10 doctoral students right now, which seems peculiar for someone who is supposed to be half-retired.

Forney: Any final words of wisdom?

Gallager: Well, I guess one piece of wisdom that I've picked up over the years is not only to listen to wise people whom I respect, but also to listen to myself even more carefully. You can't do good research unless you have insight. If you're doing something suggested by somebody else, then you probably won't have much insight about it. You really have to pick your own problem, and you have to play with it and think about it on your own. If you listen to other people to learn what's important, they usually don't know. All the wise men were saying that communication theory was dead in 1970. 1970 was probably the time when the largest number of new communication applications were really starting to happen. It was the worst possible time to get out of the field. And I think that this is true throughout technology. Many people who forecast technology are beyond their most productive years, and are not the people who ought to be trying to figure out where the field is going.

Forney: Thank you very much. Have a great trip!

Conference Calendar

DATE	CONFERENCE	LOCATION	CONTACT/INFORMATION	DUE DATE
September 22-24, 1999	37-th Annual Allerton Conference on Communication, Control, and Computing	Monticello, Illinois, USA	37-th Annual Allerton Conference Coordinated Science Laboratory University of Illinois 1308 W. Main Street Urbana, Illinois 61801-2307 USA Email: allerton@csl.uiuc.edu Web: http://www.comm.csl.uiuc.edu/allerton/	
November 5-7, 1999	Midwest Arithmetical Geometry Cryptography (MAGC) Workshop	University of Illinois, Urbana, Illinois, USA	http://www.math.uiuc.edu/~boston/magc.html	
November 9-12, 1999	DIMACS Workshop on Codes and Association Schemes	DIMACS Center, Rutgers University, Piscataway, NJ, USA	Alexander Barg Lucent Technologies Email: abarg@research.bell-labs.com Simon Litsyn Tel Aviv University Email: litsyn@eng.tau.ac.il Web: http://dimacs.rutgers.edu/ Workshops/AssociationSchemes/	
November 9-13, 1999	The Third International Conference on Distributed Computer Communication Networks (DCCN'99)	Tel Aviv, Israel	Dr. Nina Bakanova Fax: (7 095)-209-0579 Email: nina@iitp.ru Web: http://www.iitp.ru/dccn	
November 14-19, 1999.	13th AAECC Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes	Honolulu, Hawaii, USA	Prof. Marc Fossorier University of Hawaii Dept. of Electrical Engineering 2540 Dole St., # 483 Honolulu, HI 96822, USA E-mail: marc@spectra.eng.hawaii.edu Web: http://www.irit.fr/ACTIVITES/ AAECC/aaecc13.htm	

Conference Calendar

DATE	CONFERENCE	LOCATION	CONTACT/INFORMATION	DUE DATE
November 30-December 3, 1999	1999 Symposium on Information Theory and Its Applications (SITA'99)	Niigata, Japan	SITA'99 Secretariat Department of Electrical Engineering Nagaoka University of Technology Nagaoka, Niigata 940-2188, Japan Tel: +81-258-21-4263 Fax: +81-258-47-9500 Email: sita99@comm.nagaokaut.ac.jp Web: http://comm.nagaokaut.ac.jp/SITA99/	September 5, 1999
January 17-19, 2000	3rd ITG Conference on Source and Channel Coding	Munich, Germany	Joachim Hagenauer Institute for Communications Engineering Technische Universitaet Muenchen D-80290 Muenchen, Germany Web: http://www.LNT.ei.tum.de/itg/itg_main.html	
March 26-30, 2000	IEEE INFOCOM 2000	Tel Aviv, Israel	Web: http://www.comnet.technion.ac.il/infocom2000 (Israel) http://www.cse.ucsc.edu/~rom/infocom2000 (USA) http://halo.kuamp.kyoto-u.ac.jp/~infocom (Japan)	
June 5-9, 2000 I	EEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2000)	Istanbul, Turkey	Conference Management Services 3109 Westchester Ave. College Station, TX, USA 77845-7919 Email: mercer@conf-mgmt.com Web: http://icassp2000.sdsu.edu	November 11, 1999
June 18-19, 2000	7th International Workshop on Algebraic and Combinatorial Coding Theory	Blagoevgrad, Bulgaria	S. M. Dodunekov Institute of Mathematics and Informatics Bulgarian Academy of Sciences 8 G. Bonchev Str. 1113 Sofia, Bulgaria Email: stedo@moi.math.bas.bg	March 31, 2000
June 25-30, 2000	**ISIT 2000**	Sorrento, Italy	Professor Ezio Biglieri Dipartimento di Elettronica Politecnico di Torino Corso Duca Degli Abruzzi, 24 I-10129, Torino, Italy email: biglieri@polito.it Tel: +39 011 5644030 Fax: +39 011 5644099 Web: http://www.unisa.it/isit2000	September 15, 1999

IEEE

Information Theory Society Newsletter

445 Hoes Lane, P.O. Box 1331
Piscataway, NJ 08855-1331 USA